FortiCASB Handbook

VERSION 1.2.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Thursday, March 15, 2018

FortiCASB Handbook 1.2

2nd Edition

TABLE OF CONTENTS

Change log

Date	Change Description
2018-03-02	FortiCASB 1.2.0 handbook initial release.
2018-03-15	Revision 1: The policy section was revised to include additional features.

Introduction

Welcome, and thank you for selecting FortiCASB for your cloud security and monitoring needs.

FortiCASB is Fortinet's cloud-native Cloud Access Security Broker (CASB) service, which provides visibility, compliance, data security, and threat protection for cloud-based services. Using direct API access, FortiCASB enables deep inspection and policy management for data stored in Software as a Service (SaaS) platforms. It also provides detailed user analytics and management tools to ensure that policies are enforced and that your organization’s data is secure.

FortiCASB works by focusing on Gartner's four pillars of security: visibility, compliance, data security, and threat protection.

- **Visibility**—Visibility is one of the most important aspects of cloud security. FortiCASB uses a series of methods such as data scans and analytics to answer the questions: who accessed information, what was accessed, when it was accessed, and from where did the access originate.
- **Compliance**—FortiCASB provides file content monitoring to find and report on regulated data in the cloud.
- **Data security**—FortiCASB runs scans to check for sensitive data, such as social security numbers or credit card numbers. It then classifies this data under different levels of sensitivity and sends different alerts depending on the sensitivity level of the data accessed.
- **Threat protection**—FortiCASB uses User Entity Behavior Analytics to watch for suspicious or irregular user behavior. It also sends out alerts for malicious behavior.

Features

FortiCASB comes with a series of features that give you visibility of data access and usage, control over data security and threat protection, and peace of mind over compliance with standards and federal regulations.

Visibility

- **On-demand data scan**—FortiCASB examines existing content in all folders to identify sensitive data subjects or security policies.
- **Cloud usage analytics**— FortiCASB visually summarizes key usage statistics, including trends over different time periods as well as drilldown, access count, and usage over time.
- **User entitlements review**— FortiCASB gives visibility of privileged users, dormant users, and external users.
- **File exposure**— FortiCASB highlights the most shared files overall, as well as each user's most shared files.

Data security and threat protection

- **Cloud data loss prevention**— FortiCASB enforces DLP policies based on data identifiers, keywords, and regular expressions for data both at rest and in traffic.
- **Threat detection**—FortiCASB offers an abundant number of out-of-the-box policies to immediately detect account-centric threats.
- **Malware detection**— FortiCASB features a malware detection policy to detect malicious files before they compromise sensitive data.
- **Geo-location analytics**—FortiCASB visualizes global access patterns and analyzes activity to identify unlikely cross-region access attempts indicative of compromised accounts.
- **Shadow IT discovery** – FortiCASB offers an overview of unsanctioned cloud applications used in the organization and gives users the ability to control application usage.

Compliance

- **Predefined compliance policies**—FortiCASB provides predefined compliance policies designed to help maintain compliance with SOX, PCI, HIPAA, and GDPR regulations.
- **Compliance report**—FortiCASB can produce compliance reports for audit purposes. These reports show compliance with SOX, PCI, HIPAA, and GDPR regulations.

Getting started

This chapter provides the procedures for getting started with FortiCASB.

To fully set up FortiCASB, you must do the following:

- Add companies and users.
- Install SaaS applications.

Adding companies and users

If you are a user, not an administrator in charge of setup, skip to the user section.

FortiCASB requires different setup procedures, depending on your organization's hierarchy and needs. A company with a branched hierarchy, such as a company with multiple branch offices or a compartmentalized organizational structure, will have different requirements than a company with only one unified office.

From the examples below, choose the scenario that best suits your requirements:

Scenario 1: You have a company without a branched hierarchy.

- See Simple setup.

Scenario 2: You have a company with a branched hierarchy.

- See Branched setup.

Scenario 3: You are a Managed Security Service Provider (MSSP) providing service to multiple companies.

- See Branched setup. Make sure the licenses are assigned to the correct companies.

Scenario 4: You are a Fortinet Sales or Service representative assisting multiple companies.

- See Branched setup. Make sure the licenses are assigned to the correct companies.

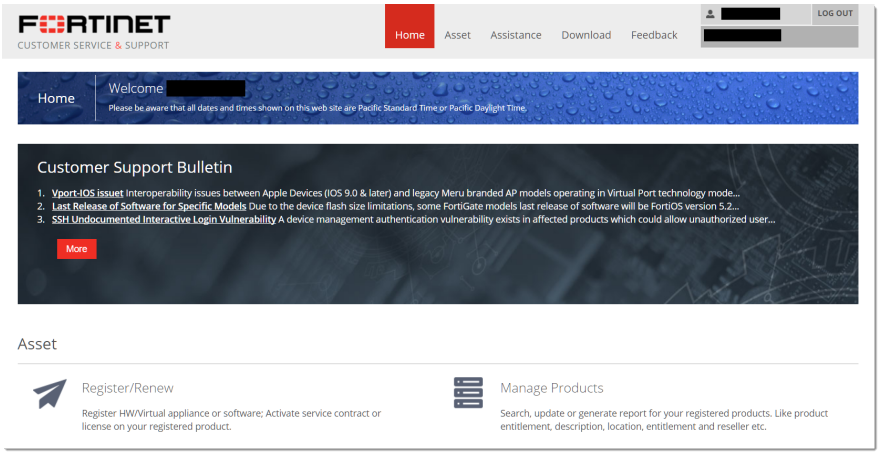
Simple setup

Before users can use FortiCASB, an administrator with a Master FortiCare account must add the company and users.

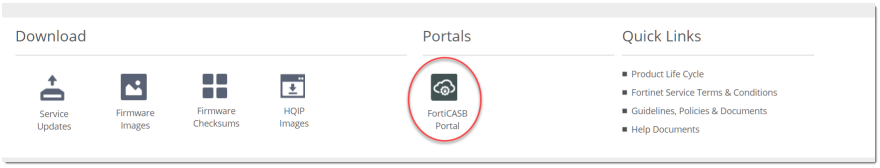
In accordance with European Union laws and regulations, all data collected by FortiCASB for European Union companies must be located in the EU region. To accommodate for this, users can choose to host their CASB cloud service either on the Global site or the EU site.

Before you log in to your account, use the menu to select either the Global or European Union region. All companies you add must be located in the same region.

1. Using a web browser, go to https://www.forticasb.com.
2. Use the drop-down menu to select either Global or European Union.
3. Click **Login**.
   You will be redirected to the Fortinet Service and Support webpage.
4. Log in to your admin account, or sign up for a new admin account.
5. Purchase a valid license for FortiCASB. Contact your primary Fortinet Service Provider for more information.
6. Log in to your account.
   You will be redirected to your Fortinet Customer Service & Support homepage.



7. Scroll down until you see the FortiCASB portal.



8. Click on this portal to be redirected to the FortiCASB GUI.

If you have a popup blocker, it will block the FortiCASB GUI. Set an exception for the FortiCASB GUI, or open the GUI manually.

Add a company

After selecting a region, the company selection screen will be displayed.

1. Click the **Add New Company** button to add a new company.
2. Enter the company name and description. The company's region is, by default, the account region selected earlier.
3. Add users to the company using their FortiCare accounts. These accounts should be sub-users in the Master FortiCare account.

Assign a license

4. After adding users, you can assign a license to the company. There are two concepts associated with licenses:
   - **Contract**—This is the basic license unit. A license contains at least one contract.
   - **Seat**—Each contract contains a specific number of seats. The number of seats represents the number of users a contract supports.

   In this scenario, use the **Add Asset** option to assign all contracts and seats to the company.
5. Click **Add Company** to finish creating your company.

Edit company information

After assigning a license to the company, log in to FortiCASB and confirm your company information.

1. From the company management page, select your company.
   It will bring you to the FortiCASB dashboard.
2. Click the **Company Setting** button, located at the top-right.
   The Company Setting page will appear. Use this to edit users or contracts.

Log in as a user

1. Go to https://www.forticasb.com.
2. Select a region and click **Login**.
3. Enter your FortiCare account credentials, then select your FortiCare sub-user account (if applicable).
4. Select your company.
   You will be brought to the FortiCASB dashboard.

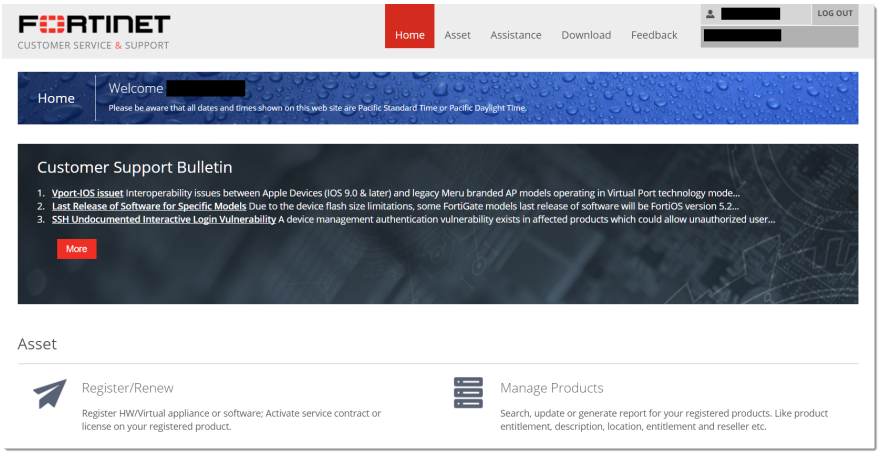
Branched setup

Before users can use FortiCASB, an administrator with a Master FortiCare account must add the company and users.

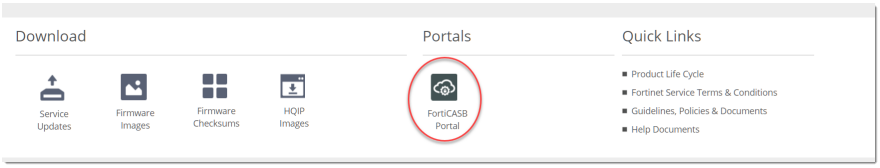
In accordance with European Union laws and regulations, all data collected by FortiCASB for European Union companies must be located in the EU region. To accommodate for this, users can choose to host their CASB cloud service either on the Global site or the EU site.

Before you log in to your account, use the menu to select either the Global or European Union region. All companies you add must be located in the same region.

1. Using a web browser, go to https://www.forticasb.com.
2. Use the drop-down menu to select either Global or European Union.
3. Click **Login**.
   You will be redirected to the Fortinet Service and Support webpage.
4. Log in to your admin account, or sign up for a new admin account.
5. Purchase a valid license for FortiCASB. Contact your primary Fortinet Service Provider for more information.
6. Log in to your account.
   You will be redirected to your Fortinet Customer Service & Support homepage.



7. Scroll down until you see the FortiCASB portal.



8. Click on this portal to be redirected to the FortiCASB GUI.

If you have a popup blocker, it will block the FortiCASB GUI. Set an exception for the FortiCASB GUI, or open the GUI manually.

Add a company

After selecting a region, the company selection screen will be displayed.

1. Click the **Add New Company** icon to add a new company.
2. Enter the company name and description. The company's region is, by default, the account region selected earlier.
3. Add users to the company using their FortiCare accounts. These accounts should be sub-users in the Master FortiCare account. The same user can be added to multiple companies.

Assign a license

4. After adding users, you can assign a license to the company. There are two concepts associated with licenses:
   - **Contract**—This is the basic license unit. A license contains at least one contract.
   - **Seat**—Each contract contains a specific number of seats. The number of seats represents the number of users a contract supports.

   In this scenario, use the **Add Asset** option to assign contracts and seats to each company as necessary. You can assign a contract and all its seats to one company, or split a contract between companies.
5. Click **Add Company** to finish creating your company.
6. Repeat steps 1-5 to add additional companies.

Edit company information

After creating your companies, log in to FortiCASB and confirm company information for each company.

1. From the company management page, select your company.
   It will bring you to the FortiCASB dashboard.
2. Click the **Company Setting** button, located at the top-right.
   The Company Setting page will appear. Use this to edit users or contracts.
3. Repeat this process for each company.

Log in as a user

1. Go to https://www.forticasb.com.
2. Select a region and click **Login**.
3. Enter your FortiCare account credentials, then select your FortiCare sub-user account (if applicable).
4. Select your company.

   You will be brought to the FortiCASB dashboard. Click on the **Switch Company** icon to switch companies, if applicable.

Installing SaaS applications

Both administrators and users can add SaaS applications to a company. Once added, everyone in the company can see the application.

Salesforce

FortiCASB offers an API-based approach, pulling data directly from Salesforce via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- Enterprise Edition
- Unlimited Edition
- Developer Edition
- Performance Edition

The user account installed in FortiCASB must have the following permissions:

- View All Data
- View All Users
- API Enabled

You may either use an existing account or create a new account. If you create a new account, wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

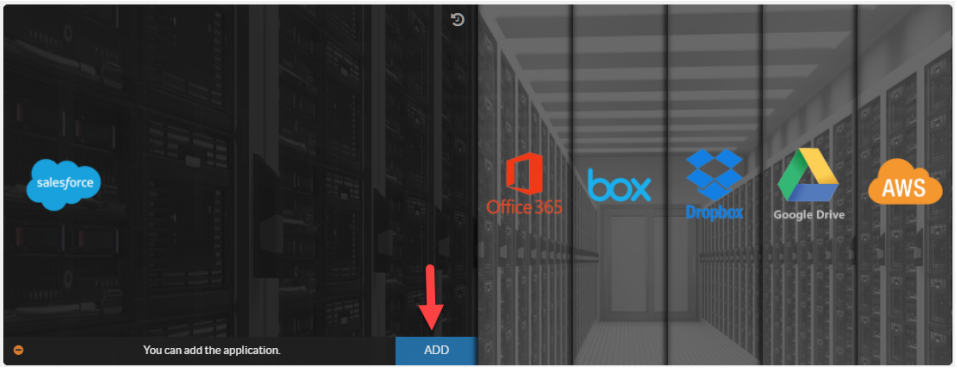
The following features require "Manage Users" permission as well:

- User login tracking
- User IP address tracking
- Geographical location tracking
- User password change tracking

Without "Manage Users" permissions, FortiCASB cannot obtain user login IPs. Therefore, any user activity will not appear on the Activity map.

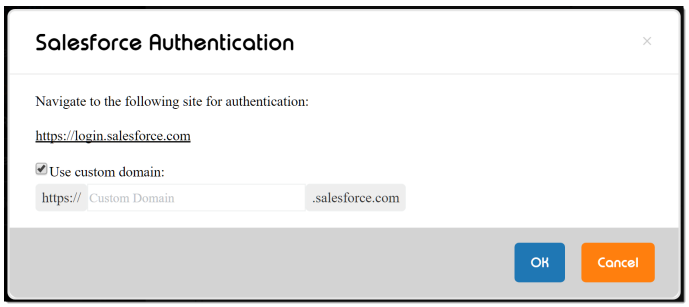
Installation

1. From the menu on the left-hand side, select **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Salesforce.



3. Click **OK**.
   You will be navigated to the Salesforce website for authentication.

   If you have a custom Salesforce domain, enter it here.



4. Log in to authenticate.
   Salesforce will prompt you to allow or deny access.
5. Click **Allow** to grant FortiCASB permissions to monitor your Salesforce application.
   After you click Allow, you will be redirected back to the FortiCASB dashboard.

   You can check the installation result and SaaS platform monitoring status in the Salesforce dashboard.

For more information on common installation issues, see "Troubleshooting" on page 68.

Office 365

FortiCASB offers an API-based approach. It monitors Office 365 activity by using web notification and by pulling data directly from Office 365 via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

You may use an existing account or create a new account. If you create a new account, wait for at least 24 hours for the new account to take effect before granting access to FortiCASB.

Make sure your role is "Global Administrator" and that you have the AzureAD "Premium P2" license. Without the AzureAD "Premium P2" license, FortiCASB's Discovery feature cannot see user entitlements. All other functions will not be affected. For more information on how to obtain this license, go to: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-get-started-premium.

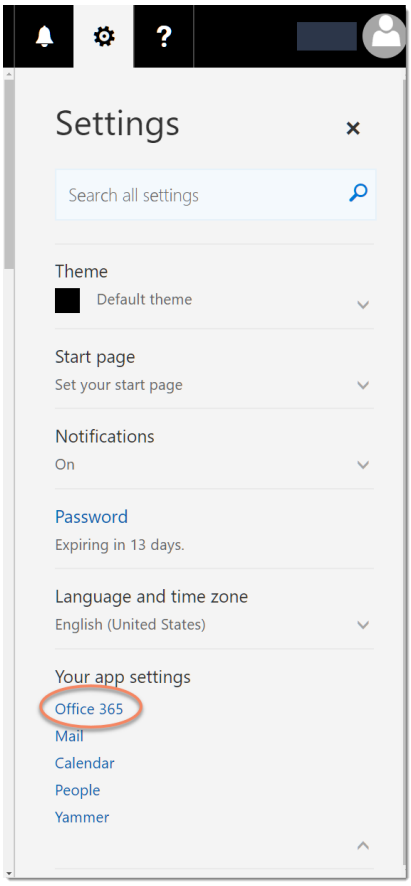
You will also need to set up the AzureAD Privileged Identity Management application. For more information on how to do so, go to: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-privileged-identity-management-getting-started.

Make sure your license plan includes Active Directory integration. FortiCASB requires Active Directory support for most of its features. The following Office 365 licenses support Active Directory integration:

- Office 365 Business
- Office 365 Business Essentials
- Office 365 Business Premium
- Office 365 ProPlus
- Office 365 Enterprise E1
- Office 365 Enterprise E3
- Office 365 Enterprise E5
- Office 365 Enterprise K1

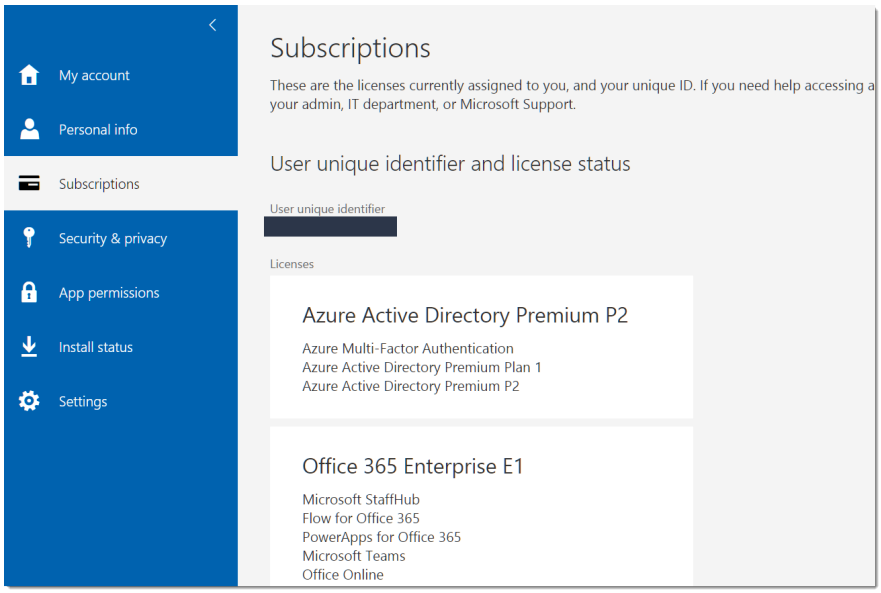
To determine what Office 365 license you have, follow the steps below:

1. Click the Settings button, located on the top-right corner of your Office 365 home screen.
2. Click **Office 365**, located under "Your app settings".



You will be redirected to your Office 365 Account page.

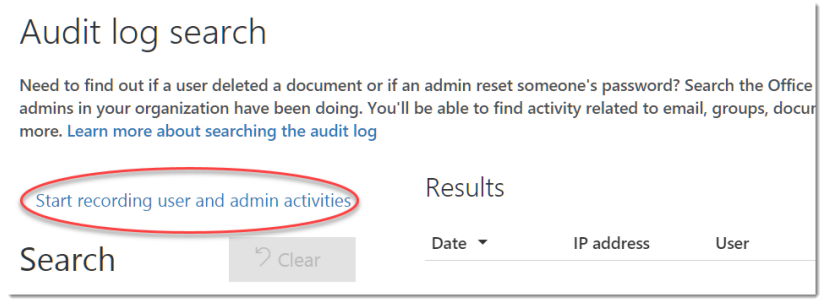
3. Click **Subscriptions** from the list on the left.
   It will display your Office 365 License, along with your Azure Active Directory Premium P2 license, if you have it purchased.



You must also allow Office 365 to record user and admin activities. To enable this feature, follow the steps below:

1. Click **Security & Compliance**, from your Office 365 home screen.

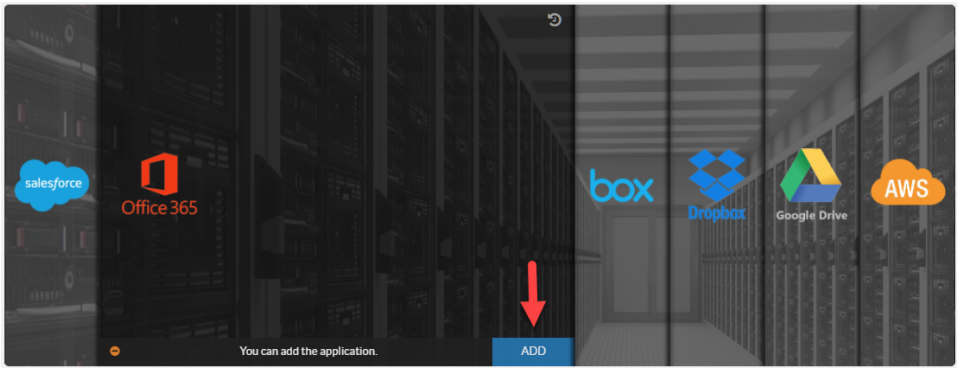
2. Click **Search & investigation**, from the menu on the left-hand side.
3. Click **Audit log search**.
4. Click **Start recording user and admin activities**.



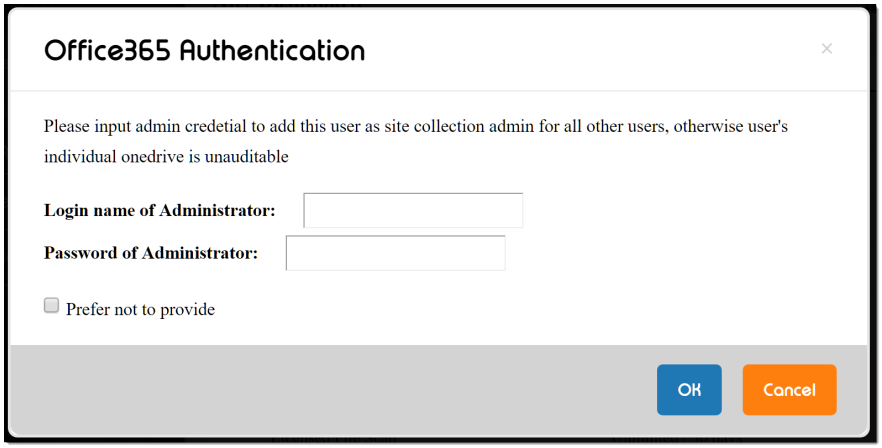
FortiCASB will now be able to monitor Office 365 activity.

Installation

1. Go to **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Office 365.



You will be prompted to provide administrator credentials. FortiCASB will use this information to add this administrator as the "site collection administrator" of all Office 365 users in the company. This is necessary for FortiCASB to audit files stored inside each user's individual OneDrive.



If you don't want FortiCASB to audit users' OneDrives, or just want to do it manually, you can check "Prefer not to provide".

If you have a custom SharePoint homepage URL, you will have to allow collection manually.

See "Troubleshooting" on page 68 for more information.

3. Click **OK**.
   You will be redirected to the Office 365 login screen.

   After logging in, Office 365 will prompt you to allow or deny FortiCASB access.
4. Click **Allow** to grant FortiCASB permissions required to monitor your Office 365 application.
   You will be redirected back to the FortiCASB dashboard.

You can check the installation result and SaaS platform monitoring status in the Office 365 dashboard.

Box

FortiCASB offers an API-based approach, pulling data directly from Box via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- Business Edition
- Enterprise Edition
- Developer Edition

The user account installed in FortiCASB must have the following permissions:

- Read and write all files and folders stored in Box
- Manage users
- Manage groups
- Manage enterprise properties

You may either use an existing account or create a new account. If you create a new account, wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

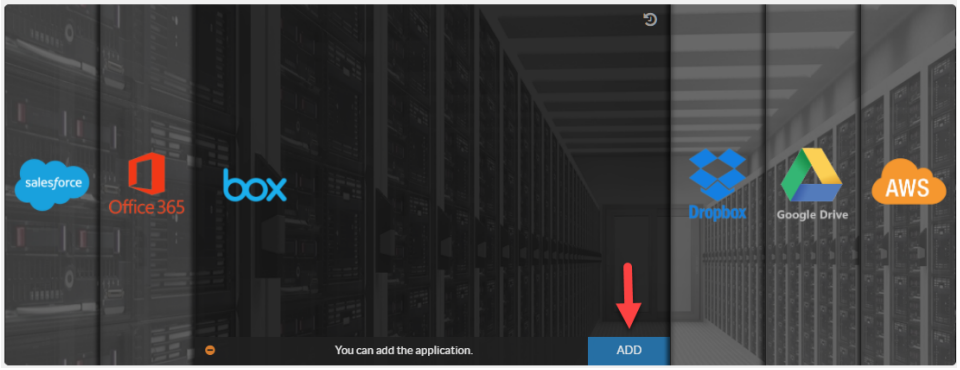
The following features require "Admin User" permission as well:

- User login tracking
- User IP address tracking
- Geographical location tracking
- User password change tracking
- Change admin role tracking

Without "Admin User" permissions, FortiCASB cannot obtain user login IPs. Therefore, any user activity will not appear on the Activity map.

Installation

1. From the menu on the left-hand side, select **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Box.



3. Click **OK**.
   You will be navigated to the Box website for authentication.
4. Log in to authenticate.
   Box will prompt you to allow or deny access.
5. Click **Allow** to grant FortiCASB permissions to monitor your Box application.
   After you click Allow, you will be redirected back to the FortiCASB dashboard.

   You can check the installation result and SaaS platform monitoring status in the Box dashboard.

For more information on common installation issues, see "Troubleshooting" on page 68.

Dropbox Business

FortiCASB offers an API-based approach, pulling data directly from Box via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following Dropbox Business plans:

- Standard Plan
- Advanced Plan
- Enterprise Plan

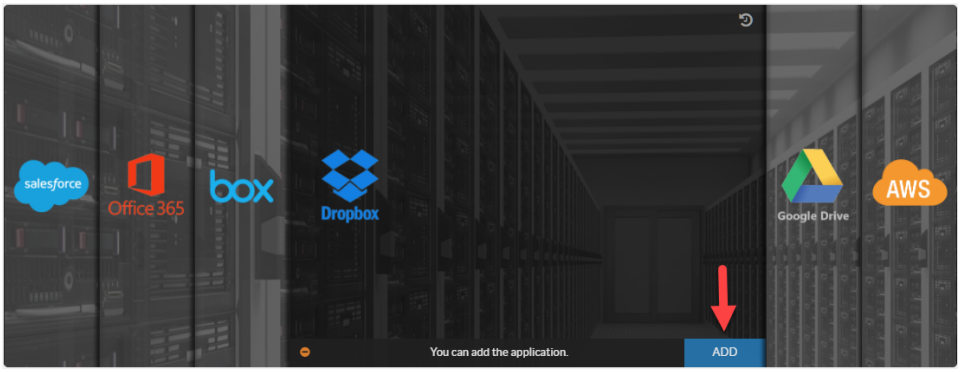
The user account installed in FortiCASB must have the following permission:

- Team Admin

You may either use an existing account or create a new account.

Installation

1. From the menu on the left-hand side, select **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Dropbox.



3. Click **OK**.
   You will be navigated to the Dropbox website for authentication.
4. Log in to authenticate.
   Dropbox will prompt you to allow or deny access.
5. Click **Allow** to grant FortiCASB permissions to monitor your Dropbox application.
   After you click Allow, you will be redirected back to the FortiCASB dashboard.

   You can check the installation result and SaaS platform monitoring status in the Dropbox dashboard.

For more information on common installation issues, see "Troubleshooting" on page 68.

Google Drive

FortiCASB offers an API-based approach, pulling data directly from Google Drive via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

To use API access, your organization must be using one of the following editions (the API is enabled by default):

- Business Edition
- Enterprise Edition

The user account installed in FortiCASB must be a Super Administrator in your G suite account. For steps on how to check if your account is a Super Adminstrator, see "Google Drive connection errors" on page 73.

Due to Google requirements, only G Suite accounts with a business or enterprise license can use FortiCASB. G suite accounts with a basic license will be unable to use FortiCASB.

You may either use an existing account or create a new account. Wait at least 24 hours for the new account to take effect before granting access to FortiCASB.

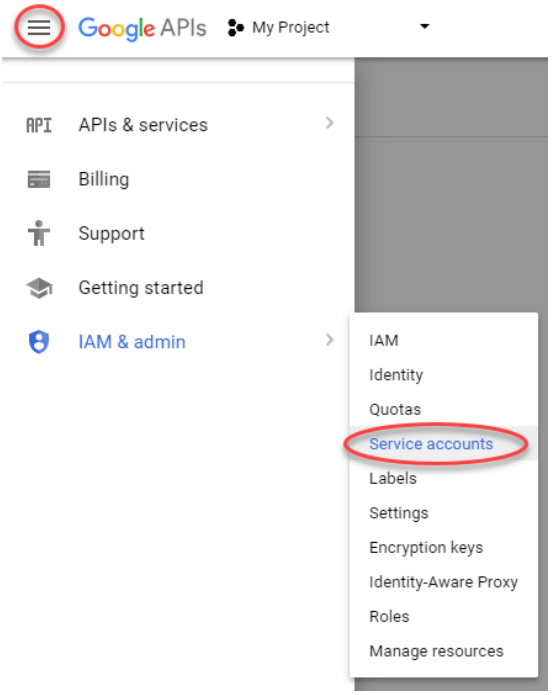
Make sure you create a service account for the G Suite account that will be linked to FortiCASB. A service account delegated with domain-wide authority is necessary for FortiCASB to visit files in both personal and team drives under your G Suite account.

Without the service account, you can still use FortiCASB. However, the features related to files in FortiCASB, such as Discovery, will not work.

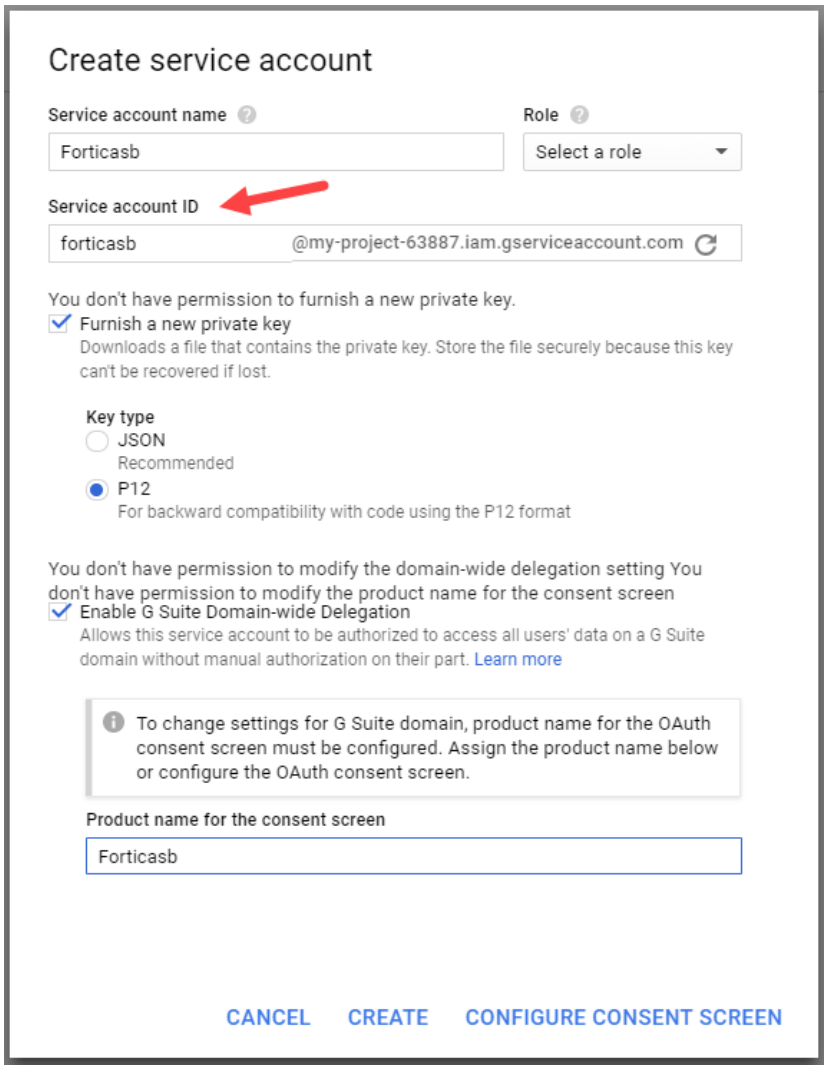
For more information regarding service accounts and domain-wide authority delegation, go to: https://developers.google.com/identity/protocols/OAuth2ServiceAccount#delegatingauthority.

To create a service account, follow the steps below:

1. Go to https://console.developers.google.com and log in with your Google Account.
2. Create a project.
3. From the "Products and services" menu, go to **IAM & admin > Service accounts**.



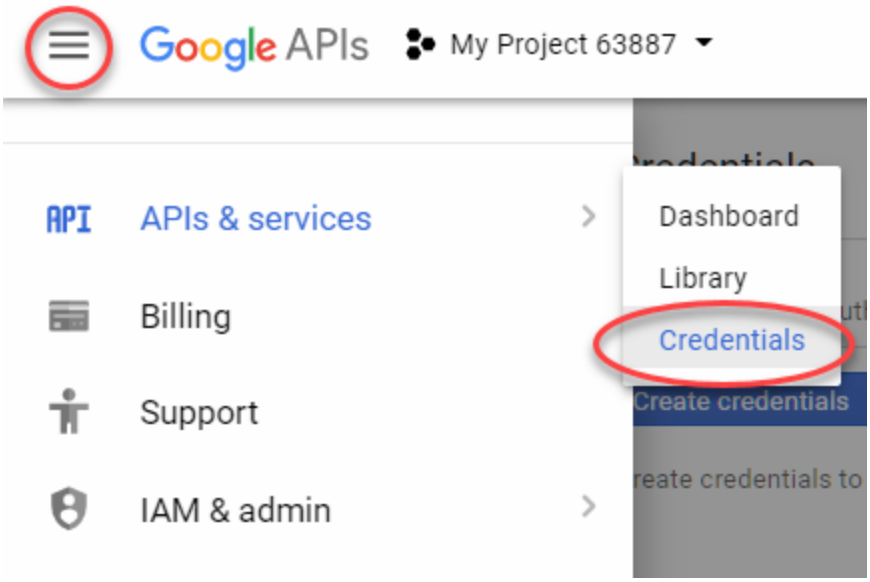
4. Click **Create service account**.
5. Enter in a "Service account name" and a "Service account ID".
6. Enable "Furnish a new private key" and select P12.
7. Enable "G Suite Domain-wide Delegation" and enter in a "Product name for the consent screen". The red arrow points to your Service Account ID. The red arrow points to your Service Account ID.



8. Click **CREATE**. The P12 private key will be downloaded automatically.

Keep this key and your service account ID for future use.

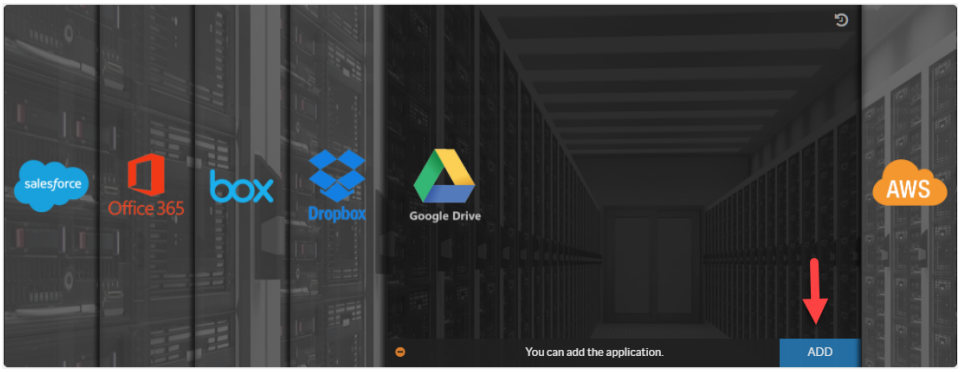
9. Go to **APIs & Services > Credentials**.



10. Find and write down the "Client ID".
11. Go to **APIs & Services > Dashboard**.
12. Click **ENABLE APIS AND SERVICES**.
13. Search for the "Google Drive API" and enable it.
14. Go to https://admin.google.com and log in with the same Google Account.
15. Go to **Security > Advanced Settings**.
16. Click **Manage API client access**.
17. In step 6, enter in the Client ID for "Client Name" and "https://www.googleapis.com/auth/drive" for "One or More API Scopes". Your Client ID should be a string of numbers.

Installation

1. From the menu on the left-hand side, select **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to Google Drive.



3. Upload the service account ID and Private Key (P12 File) for the G suite account. Your service account ID should end in ".gserviceaccount.com".
4. Click **OK**.

You will be navigated to the Google website for authentication. Make sure to use the same G suite account for authentication.

If you have a custom Google domain, enter it here.

5. Log in to authenticate.
   Google will prompt you to allow or deny access.
6. Click **Allow** to grant FortiCASB permission to monitor your Google application.
   You will be redirected back to the FortiCASB dashboard. You can check the installation result and SaaS platform monitoring status in the Google Drive dashboard.

Amazon Web Services

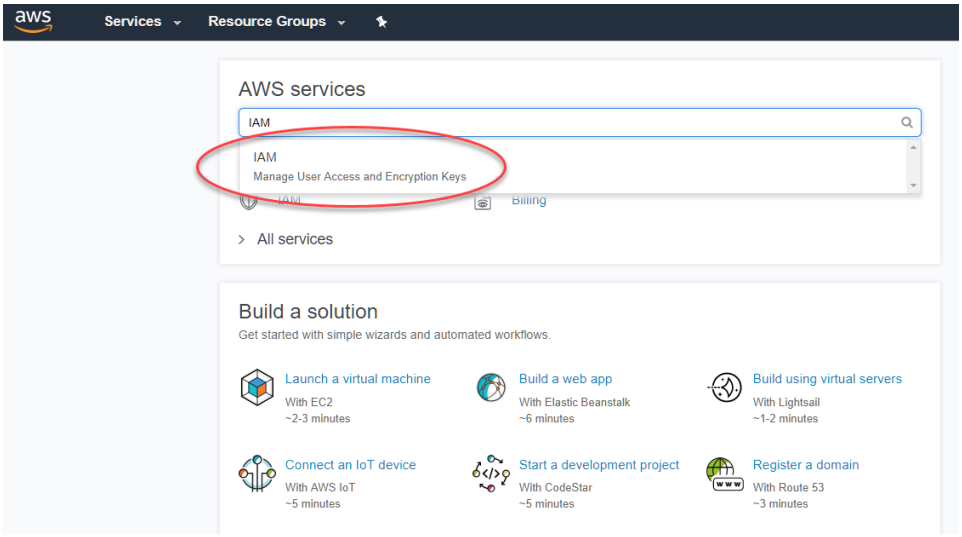
FortiCASB offers an API-based approach, pulling data directly from AWS via RESTful API. Authentication is done through OAUth2.0. FortiCASB uses an access token for API queries.

Prerequisites

You must create a new role in your AWS account for FortiCASB before using FortiCASB with AWS.

To create a role, use the following steps:

1. Go to your AWS console dashboard.
2. Search and click **IAM**.



3. Click **Policies** from the menu on the left.
4. Click **Create policy**.
5. Go to the JSON tab.
6. Replace the existing JSON code with the following:

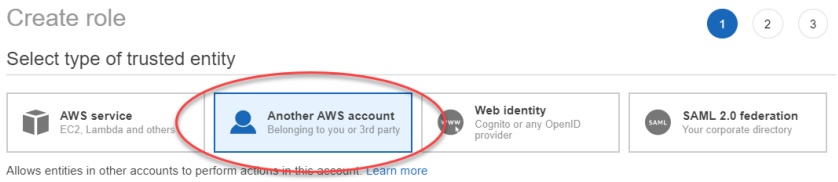
```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
```

```
"appstream:Describe*",
"config:Get*",
"iam:List*",
"cloudtrail:GetTrailStatus",
"route53:GetHealthCheck",
"cloudfront:Get*",
"guardduty:List*",
"codedeploy:List*",
"cloudwatch:Describe*",
"route53:ListHostedZonesByName",
"config:Describe*",
"s3:ListObjects",
"datapipeline:EvaluateExpression",
"iam:SimulateCustomPolicy",
"rds:Describe*",
"ec2:ModifySnapshotAttribute",
"ec2:RevokeSecurityGroupEgress",
"rds:DownloadDBLogFilePortion",
"s3:GetBucket*",
"route53:GetHostedZoneCount",
"logs:FilterLogEvents",
"inspector:Describe*",
"acm:List*",
"config:Deliver*",
"cloudfront:List*",
"s3:GetIpConfiguration",
"cloudtrail:LookupEvents",
"route53:GetHealthCheckLastFailureReason",
"datapipeline:ListPipelines",
"lambda:List*",
"sqs:SendMessage",
"kms:Describe*",
"logs:Get*",
"s3:GetReplicationConfiguration",
"cloudtrail:DescribeTrails",
"ec2:RevokeSecurityGroupIngress",
"route53:ListTagsForResources",
"s3:PutObjectVersionAcl",
"waf:List*",
"workspaces:Describe*",
"redshift:ModifyClusterParameterGroup",
"glacier:ListVaults",
"elasticloadbalancing:ModifyLoadBalancerAttributes",
"iam:GenerateCredentialReport",
"s3:GetLifecycleConfiguration",
"tag:GetResources",
"s3:GetInventoryConfiguration",
"acm:Describe*",
"cloudtrail:StartLogging",
"route53domains:ListTagsForDomain",
"dynamodb:ListTables",
"sns:ListTopics",
"s3:ListBucket",
"route53domains:GetDomainDetail",
"datapipeline:ValidatePipelineDefinition",
"datapipeline:DescribePipelines",
"elasticmapreduce:List*",
```

```
"iam:Get*",
"route53:GetCheckerIpRanges",
"route53domains:ListDomains",
"route53:GetGeoLocations",
"route53:ListGeoLocations",
"kms:EnableKeyRotation",
"s3:ListBucketMultipartUploads",
"cloudsearch:Describe*",
"ecs:Describe*",
"route53:ListHostedZones",
"datapipeline:QueryObjects",
"guardduty:Get*",
"elasticache:Describe*",
"route53:ListTagsForResource",
"ec2:Describe*",
"directconnect:Describe*",
"route53:ListHealthChecks",
"codedeploy:Get*",
"rds:ListTagsForResource",
"s3:ListAllMyBuckets",
"route53domains:ListOperations",
"s3:GetObjectVersion",
"kms:List*",
"glacier:GetVaultAccessPolicy",
"logs:Describe*",
"s3:GetObjectVersionTagging",
"route53:GetHostedZone",
"kms:Get*",
"ses:List*",
"s3:GetObjectAcl",
"iam:SimulatePrincipalPolicy",
"codedeploy:Batch*",
"dynamodb:DescribeTable",
"cloudtrail:ListTags",
"route53:ListResourceRecordSets",
"s3:GetObjectVersionAcl",
"rds:ModifyDBInstance",
"s3:PutBucketAcl",
"elasticloadbalancing:Describe*",
"cloudformation:ListStack*",
"s3:HeadBucket",
"es:Describe*",
"route53:GetHealthCheckCount",
"sdb:DomainMetadata",
"route53:ListReusableDelegationSets",
"ses:Get*",
"elasticfilesystem:Describe*",
"sqs:GetQueueAttributes",
"elasticbeanstalk:Describe*",
"route53domains:GetOperationDetail",
"s3:ListMultipartUploadParts",
"s3:GetObject",
"iam:UpdateAccountPasswordPolicy",
"redshift:Describe*",
"cloudformation:GetTemplate",
"s3:GetAnalyticsConfiguration",
"s3:GetObjectVersionForReplication",
```

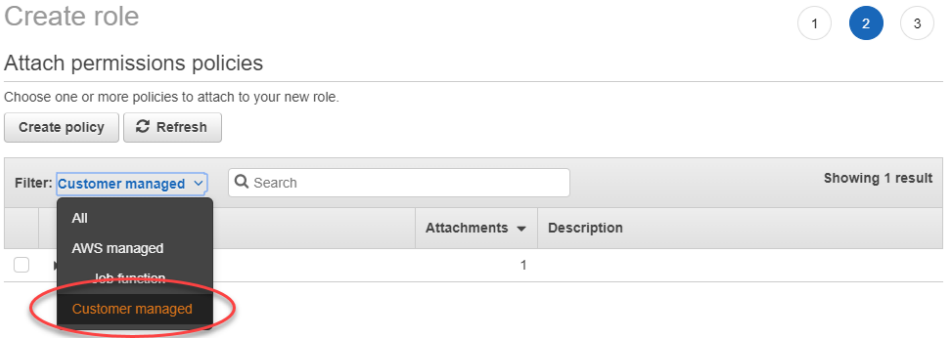
```
                "autoscaling:Describe*",
                "s3:ListBucketByTags",
                "route53:GetChange",
                "s3:ListBucketVersions",
                "s3:GetAccelerateConfiguration",
                "tag:GetTagKeys",
                "s3:GetObjectVersionTorrent",
                "s3:GetEncryptionConfiguration",
                "sns:Get*",
                "elasticache:List*",
                "elasticmapreduce:ListClusters",
                "s3:GetObjectTagging",
                "s3:GetMetricsConfiguration",
                "waf:Get*",
                "ecs:List*",
                "s3:PutObjectAcl",
                "sqs:ListQueues",
                "cloudtrail:UpdateTrail",
                "ds:Describe*",
                "datapipeline:DescribeObjects",
                "route53:GetReusableDelegationSet",
                "datapipeline:GetPipelineDefinition",
                "inspector:List*",
                "sdb:ListDomains",
                "cloudformation:DescribeStack*",
                "s3:GetObjectTorrent",
                "s3:PutBucketPolicy",
                "es:List*",
                "elasticmapreduce:DescribeJobFlows",
                "lambda:GetPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

7. Click **Review policy**.
8. Name the new policy.
9. Click **Create policy**.
   Your new policy will be created.
10. Click **Roles** from the menu on the left.
11. Click **Create role**.
12. Click **Another AWS account**.

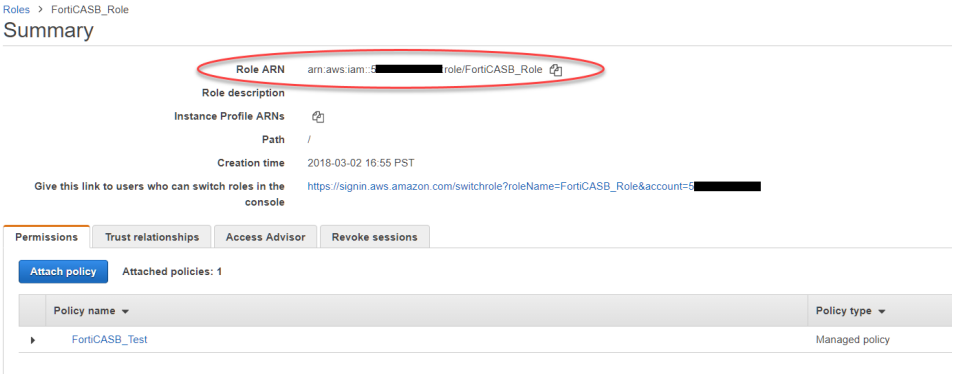


13. Enter the following Account ID: `854209929931`.
14. Select the box for Require external ID and enter in an external ID. You will need this external ID later.
15. Make sure the box for Require MFA is not selected.
16. Click **Next: Permissions**.

17. Click **Filter**, then select Customer managed.

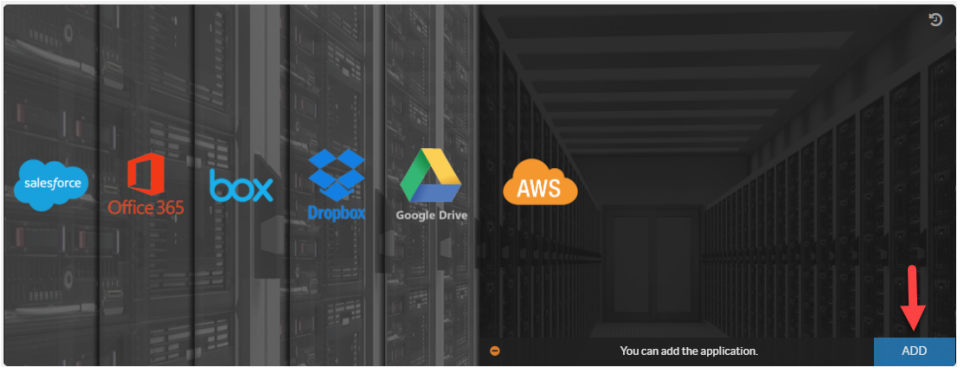


18. Select the box for the policy you created earlier.
19. Click **Next: Review**.
20. Enter a name for the role.
21. Click **Create role**.
22. Click the role name, and copy the AWS Role ARN. You will need this later.



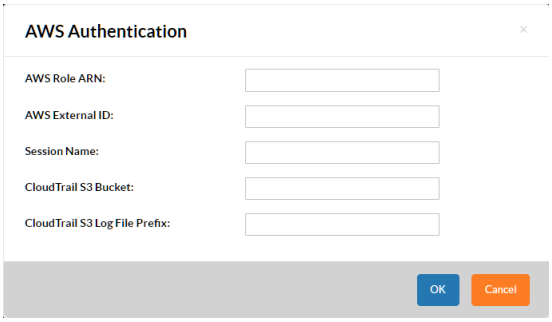
Installation

1. From the menu on the left-hand side, select **Overview > Dashboard**.
2. From the Cloud App Status widget, click **ADD**, located next to AWS.



3. You will be prompted for your AWS authentication information.

a. Enter in the AWS Role ARN you copied eariler.
b. Enter in the AWS External ID you set earlier.
c. Enter in a session name. Actions FortiCASB performs in AWS will be under this session name.
d. Both CloudTrail entries are optional.

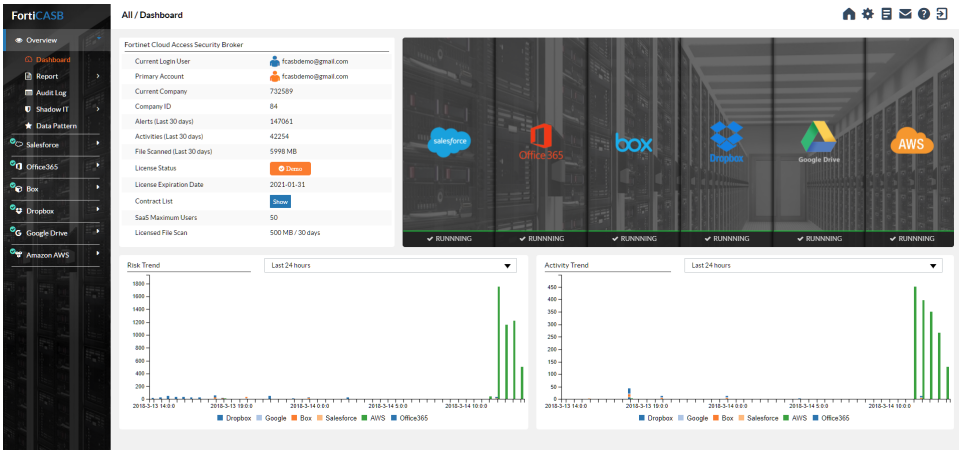


4. Click **OK**.
   You can check the installation result and SaaS platform monitoring status in the AWS dashboard.

Checking SaaS monitoring status

FortiCASB starts to monitor immediately after the SaaS has been successfully installed. To check if FortiCASB is monitoring, look for the green [Running] indicator on the SaaS panel. If an error occurs, the light will turn red, and the SaaS panel will guide you through the troubleshooting process.

Using FortiCASB



FortiCASB classifies data as either data at rest or traffic data. Data at rest is data uploaded onto the SaaS platform before it has been linked with FortiCASB, while traffic data is any data uploaded after FortiCASB has started monitoring the SaaS platform.

Data at rest

You can run scans on the data in your SaaS platforms to determine their contents. Depending on the policies you set, FortiCASB will classify this data as either sensitive data or non-sensitive data. This can be seen in the Discovery section for each SaaS platform.

If you don't run a manual scan, FortiCASB will scan files on an individual basis whenever a user accesses the file.

For more information on policies, see "Policies" on page 33.

For detailed instructions on how to run and view scans, see "On-demand data at rest scan" on page 41.

For an explanation of the panels on the Discovery page, see "Discovery" on page 42.

For more details explaining the Document page, see "Documents" on page 53.

Traffic data

Activity

FortiCASB monitors user and data traffic for your SaaS platform. This is shown in the activity page.

For more information on what is monitored and logged as activity, see "Activity" on page 45.

For more information on how FortiCASB monitors users, see "Users" on page 54.

Alerts

FortiCASB sends you alerts when one of your set policies are triggered.

- DLP policies pertain to the types of data stored in the SaaS platform.
- Threat protection policies pertain to suspicious user activity.
- Compliance policies pertain to specific regulations, such as HIPAA, PCI, and SOX.

See "Policies" on page 33 for specific policy descriptions.

Dashboard

For a description of the panels on the dashboard for each SaaS platform, see "Dashboard" on page 55.

Reports

FortiCASB allows you to generate reports. See "Reports" on page 56 for more information.

Audit log

FortiCASB records all administrator activities. You can filter your searches by using the Filter option. To access the Audit log page, go to **Overview > Audit log**.

Shadow IT discovery

When integrated with FortiGate or FortiAnalyzer, FortiCASB is able to provide an overview of all sanctioned and unsanctioned cloud applications throughout your organization. See "Shadow IT discovery" on page 57 for more information.

Data pattern

FortiCASB uses data patterns to create policies for monitoring files. You can create customized data patterns from the Data Pattern page. See "Data pattern" on page 65 for more information.

Configuration

FortiCASB provides policies that check to see if your SaaS platform is following best practices. See "Configuration" on page 66 for more information.

Buckets

FortiCASB allows you to monitor Buckets in your AWS platform. To access the Buckets page, go to **Amazon AWS > Buckets** from the navigation menu on the left.

Logs

FortiCASB accesses your information by downloading files, scanning the downloads, then subsequently deleting the downloads at regular intervals.

NOTE: For your privacy, FortiCASB does not retain your files. You may check to see when and which files FortiCASB has downloaded, scanned, and deleted by clicking the Logs button, located at the top-right corner.

Policies

FortiCASB uses policies for two purposes:

- Scans and reports use policies you set to differentiate between sensitive and non-sensitive data.
- Alerts are generated depending on the policies you set.

Default policies

FortiCASB offers Data Analysis (DA) policies, Threat Protection policies, Compliance policies, and Customized policies.

Data Analysis

DA policies keep track of sensitive data. For example, if a user accesses a file containing Social Security Numbers (SSNs) and you have the SSN policy set, FortiCASB will send you an alert.

File types supported for DA scans

Uncompressed	Microsoft Word Document (.doc, .docx)
	Microsoft Powerpoint Document (.ppt, .pptx)
	Microsft Excel Document (.xls, .xlx)
	Text File (.txt, .rtf)
Compressed	.zip
	.tar
	.7z
	.gz

DA policies

Data Analysis policies trigger alerts whenever a monitored file is accessed, regardless of the type of access. If you only want alerts for specific actions, set a Customized policy.

Identity number

US SSN Policy	FortiCASB scans for SSNs during Discovery scans, and triggers an alert when targets with SSNs are accessed.
CN Resident Identity Policy	FortiCASB scans for CN resident identity numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Credit card number

Visa Credit Card Policy	FortiCASB scans for Visa credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
MasterCard Policy	FortiCASB scans for MasterCard credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
American Express Policy	FortiCASB scans for American Express credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
Diners Club Card Policy	FortiCASB scans for Diners Club credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
Discover Card Policy	FortiCASB scans for Discover credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
JCB Policy	FortiCASB scans for JCB credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
Maestro Card Policy	FortiCASB scans for Maestro credit card numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Driver license number

UK Driver License Policy	FortiCASB scans for UK driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
US-FL Driver License Policy	FortiCASB scans for FL driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
US-CA Driver License Policy	FortiCASB scans for CA driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
CN Driver License Policy	FortiCASB scans for CN driver license numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Email address

Email Address Policy	FortiCASB scans for email addresses during Discovery scans, and triggers an alert when targets with email addresses are accessed.

Insurance number

CA Insurance Number Policy	FortiCASB scans for CA insurance numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
UK Insurance Number Policy	FortiCASB scans for UK insurance numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Passport number

UK Passport Number Policy	FortiCASB scans for UK passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
CN Passport Number Policy	FortiCASB scans for CN passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
USA/Germany Passport Number Policy	FortiCASB scans for USA/Germany passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
AU Passport Number Policy	FortiCASB scans for AU passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
JP Passport Number Policy	FortiCASB scans for JP passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
CA Passport Number Policy	FortiCASB scans for CA passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.
FR Passport Number Policy	FortiCASB scans for FR passport numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

Bank account number

China Union Pay Policy	FortiCASB scans for China Union Pay account numbers during Discovery scans, and triggers an alert when targets with such numbers are accessed.

UK IBAN Policy	FortiCASB scans for UK IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Swiss IBAN Policy	FortiCASB scans for Swiss IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
German IBAN Policy	FortiCASB scans for German IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Italian IBAN Policy	FortiCASB scans for Italian IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Swedish IBAN Policy	FortiCASB scans for Swedish IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.
Spanish IBAN Policy	FortiCASB scans for Spanish IBANs during Discovery scans, and triggers an alert when targets with such IBANs are accessed.

Birthdate

Birthdate Policy	FortiCASB scans for birthdates during Discovery scans, and triggers an alert when targets with birthdates are accessed.

Malware

AV Scan Policy	FortiCASB scans for malware during Discovery scans, and triggers an alert when targets with such malware are accessed. The Malware policy also examines files with the Windows Executable (.exe) extension.

Threat protection

Threat protection policies track suspicious user behavior. For example, if a user fails to enter his or her password correctly multiple times in a row and you have the Excessive Login Failures policy active, FortiCASB will send you an alert.

Threat protection policies

Access

Excessive Login Failures	Triggers an alert when the number of failed logins for a user exceeds a set threshold.
Password Change	Triggers an alert when passwords are changed.
Suspicious Movement	Triggers an alert when a change in a user's geographic location exceeds threshold parameters.
Unapproved Login Location	Triggers an alert when a user logs in from an unapproved geographic location.

Suspicious Activity

Restricted User	Triggers an alert when a monitored user performs select activities.
Suspicious IP	Triggers an alert when there is activity from a suspicious IP.
Suspicious Time	Triggers an alert when there is activity outside of work hours.
Suspicious Location	Triggers an alert when there is activity from suspicious locations.

Sensitive Activity

Sensitive Event	Triggers an alert when a sensitive event occurs.
Sensitive File	Triggers an alert when a specified sensitive file is accessed.

Abnormal Traffic

Large File Upload	Triggers an alert when a file upload exceeds a size threshold.

Compliance

Compliance policies track files relevant to specific regulations. For example, if a user accesses a file containing private heath information and you have the corresponding HIPAA policy set, FortiCASB will send you an alert.

Compliance policies

SOX-COBIT

SOX-COBIT policies help your organization track and show compliance with the Sarbanes-Oxley (SOX) Act of 2002 using COBIT guidelines. Use these policies to monitor your SaaS platforms for SOX compliance, then use the Report feature to print a report detailing compliance specifics.

PCI

PCI policies help your organization track and show compliance with the Payment Card Industry Data Security Standard (PCI DSS). Use these policies to monitor your SaaS platforms for PCI DSS compliance, then use the Report feature to print a report detailing compliance specifics.

HIPAA

HIPAA policies help your organization track and show compliance with the Health Insurance Portability and Accountability Act (HIPAA). Use these policies to monitor your SaaS platforms for HIPAA compliance, then use the Report feature to print a report detailing compliance specifics.

GDPR

GDPR policies help your organization track and show compliance with the EU General Data protection Regulation (GDPR). Use these policies to monitor your SaaS platforms for GDPR compliance, then use the Report feature to print a report detailing compliance specifics.

Customized

FortiCASB allows you to create personalized policies to suit your orgazational needs. To add a custom policy, click **Add** from the Customized tab.

Custom policies focus on two aspects, content monitoring and activity monitoring. Content monitoring is primarily used to monitor files for sensitive data. Activity monitoring is primarily used to monitor users and user activities.

The following examples illustrate how to create some common custom policies.

Example 1: To monitor all downloads of a public link containing sensitive data

To receive an alert whenever a file containing sensitive data is downloaded from a public link, use the Exposure setting along with the Data Pattern setting. For example, to monitor a Salesforce link containing a social security number:

1. Go to the **Content** tab.
2. Select **Specific Data Patterns**, on the right.
3. Click the box labeled **Data Pattern**, then select DLP SSN.
4. Click the box labeled **Exposure**, then select SALESFORCE_LINK.
5. Go to the **Activity** tab.

6. Select **Specific Events**, on the right.
7. Click the box labeled **Event**, then select Download File.
8. Configure any other settings as needed.

Example 2: To monitor all activities of a group of users

To receive an alert whenever a specific user or group of users performs any action, use the User setting. For example, to monitor a group of users:

1. Go to the **Activity** tab.
2. Select **Specific Users**, on the right.
3. Click the box labeled **User**, then select users to monitor. Alternatively, check the **Exclude** box on the right to monitor all users besides the ones selected.
4. Configure any other settings as needed.

How to set policies

1. Go to **Policy**.
2. Click the arrow next to the policy you wish to configure.
3. Configure the settings as described below.
4. Click **Save**.
   The policy you set should be active after a few minutes.

General

Name	Shows the name of the policy. Not configurable.
Status	Specify whether or not the policy is active. A policy is active when it is set to "true".
Policy Description	Shows a description of the policy. Not configurable.
Severity Level	Specify the severity level for the policy.
Policy Type	Shows the type of policy. Not configurable.

Context

Matching Threshold	Specify the minimum threshold for an alert. For example, a Credit Card Number policy with threshold set to two will trigger an alert when two or more credit card numbers are in a file.

Data Pattern Monitor Type	Specify either Monitor Activity, Risk Assessment, or both. If Monitor Activity is specified, alerts will be generated in the Alerts menu whenever targets are accessed. If Risk Assessment is specified, FortiCASB will search for the selected data pattern during Discovery scans.

Notification

Enable Email Notification	Check the box to allow FortiCASB to send an email whenever an alert is triggered.
Email Receiver	Either select a user to receive notifications, or enter in an email address.

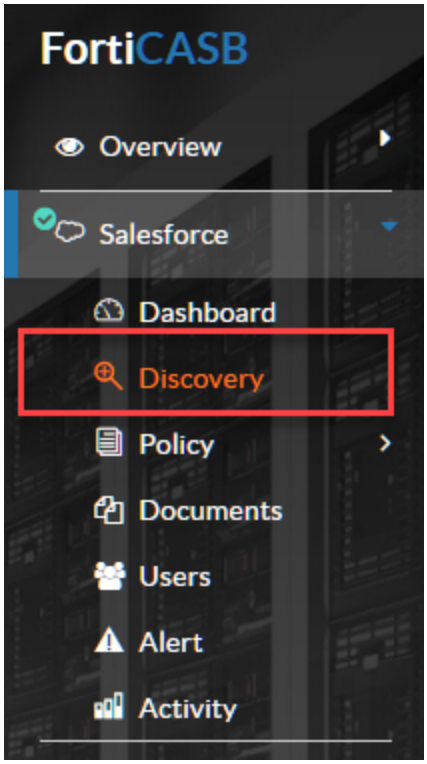
On-demand data at rest scan

FortiCASB provides an on-demand scan for data at rest. This includes sensitive data discovery based on configured DA policies, user entitlement review, and file exposure analysis.

This scan searches for and classifies data based on policies you set. For instructions on how to set those policies, as well as policy descriptions, see "Policies" on page 33.

Starting a new scan

1. Go to the Discovery Page of a SaaS platform.



2. Click the **Scan** button on the top left-hand side.

Viewing scan history

1. Click the drop-down menu on the top right-hand side.
2. Select a result from the list.

Discovery

The Discovery page shows basic information about the data in your SaaS platform, as well as information about the users with access to your data.

You may run scans from the Discovery page. For more information, see "On-demand data at rest scan" on page 41.

Panel descriptions

Overview—shows a pie chart illustrating the percentage of data in your SaaS platform that is sensitive or exposed.

User Entitlements—shows all users with access to your SaaS platform.

Privileged User	Any user with specific administrative privileges. For a list of these specific privileges, see Administrative privileges on page 43.
Dormant User	Any user that has not accessed the SaaS platform for at least 30 days.
External User	Any user from an external company with access to your SaaS platform.

If the User Entitlements panel can't get privileged roles for your Office 365 platform, make sure you have global administrator privileges and have Azure Active Directory Premium P2.

Sensitive Data Discovery—gives an overview of sensitive data on your SaaS platform.

Sensitive Files	Shows the number of files on your SaaS platform with sensitive information, out of the total number of files.
High Risk Users	Shows how many users own files with sensitive information.
Triggered Policies	Shows the number of triggered policies, out of the total number of policies set.
New Since Last Scan	Shows the number of sensitive files added since the last scan, out of the total number of sensitive files.

Click the number under Policy Violation to show the specific policies triggered.

Use **Filter** to filter or search through the list.

File Exposure—gives an overview of shared files on your SaaS platform.

Exposure Summary	Gives a summary of the file exposure. Click to filter the list.
Top File-Sharing Owners	Shows the owners sharing the most files.
Top Users/Groups with access to Shared Files	Shows the users or groups with access to the most files.

Click on […] under Share or Link for more details.

Use **Filter** to filter or search through the list.

Administrative privileges

Salesforce

A user with any of the following administrative permissions is considered a privileged user:

- Assign Permission Sets
- Manage Sharing
- Modify All Data
- Manage Encryption Keys
- View All Data
- View All Users

Office 365

A user with any of the following administrator roles is considered a privileged user:

- global administrator
- billing administrator
- password administrator
- service administrator
- user management administrator
- Exchange administrator
- SharePoint administrator
- Skype for Business administrator

Box

An admin with all of the following permissions is considered a privileged user:

- Manage users and groups
- Make calls on behalf of users
- View all data

Dropbox Business

A Team Admin is considered a privileged user.

Google

A user with any of the following administrator roles is considered a privileged user:

- Super Administrator
- Groups Administrator
- User Management Administrator
- Help Desk Administrator
- Services Administrator
- User Customized Administrator

Activity

FortiCASB tracks user activities on SaaS platforms.

The Activity page contains both a map displaying (approximate) geolocations of events and an activities list.

Map options

- **Activity**—Click on an activity indicator on the map to bring up an activity notification from that specific location.
- **Move**—Move the map by clicking a point and dragging your mouse.
- **Zoom**—Use the buttons on the bottom-right corner of the map to zoom in and out.
- **Refresh**—Click the **Refresh** button to refresh the map.
- **Clear Map**—Click the **Clear Map** button to clear the map of activity indicators.
- **Filter**—Click the **Filter** button to filter the activity notifications shown.

Raw event list

Events that come directly from a SaaS API or web notifications are displayed in Javascript Object Notation (JSON) format.

Alert correlation

One activity may trigger multiple alerts. Click the event to open the corresponding alert page.

Event list

This shows the types of events FortiCASB supports. These types of events will be traced at the activity page, and they can also be used as criteria when configuring policy and applying filters.

The File Download event is monitored within the FortiCASB Audit log. To find the audit log, go to **Overview > Audit Log** from the navigation menu on the left.

Salesforce

Login	Login Success
	Login Failed
User	Create User
	Modify User
	Change Password

	Activate User
	Deactivate User
	Change User Profile
	Change User Role
	Change User Email
	Change User Permission Set
Group	Add Group
	Add Group Member
	Update Group
	Change Group Access
	Add External Group Member (Customer)
	Invite People
Profile	Create Profile
	Modify Profile
Permission Set	Add Permission Set
	Modify Permission Set
Feed	Post
	Modify Post
	Comment
	Modify Comment
File	Upload File
	Upload New Version
	Download File
	Edit File
Share	Share File

	Share File with People
	Share File with Group
	Share File via Link
	Download File via Link
Business	Account Modification
	Account Owner Change
	Contact Modification
	Contact Owner Change
	Account Create
	Contact Create

Office 365

Login	Login Success
	Login Failed
User	Create User
	Delete User
	Modify User
	Restore User
	Change Password
	Modify Role
Group	Add Group
	Delete Group
	Add Group Member
	Update Group
	Add Group Owner
	Delete Group Owner

	Set Group Managed By
	Create Group Settings
	Update Group Settings
	Delete Group Settings
	Set Group License
File	Upload File
	Delete File
	Download File
	Modify File
	Access File
	Move File
	Copy File
	Rename File
	Edit File
Share	Share File
	Create Anonymous Link
	Delete Anonymous Link
	Create Company Link
	Delete Company Link
	Company Link Used
Other	Modify License
	Delete Folder
	Create Sharing Invitation
	Edit Company Info

Box

File/Folder	Upload File
	Copy File
	Download File
	Edit File
	Move File
	Preview File
	Rename File
	Open File
	Modify File
	Create Lock
	Comment
Login	Login Success
	Login Failed
User	Create User
	Modify User
	Delete User
Group	Add Group
	Update Group
	Group Add Membership
Metadata	Create Metadata Template
	Update Metadata Template
	Create Metadata Instance
	Update Metadata Instance
Collaboration	Collaboration Invite

	Collaboration Accept
	Collaboration Role Change
	Update Collaboration Expiration
	Collaboration Expiration
Share	Share File
	Update Shared File
	Update Shared Expiration
	Share Expiration

Dropbox Business

Login	Login Success
	Login Failed
	Logout
	Login As User Session Start
	Login As User Session End
User (Member)	Create User
	User Change Name
	User Change Status
	User Change Admin Role
	User Change Email
	Change Password
	Password Restore
	Password Restore All
Group	Add Group
	Delete Group
	Add Group Member

	Remove Group Member
	Group Rename
File	File Add
	File Download
	File Preview
	File Edit
	File Delete
	File Add Comment
	File Move
	File Copy
	File Rename
	File Restore
	File Revert
File Share	Share Link Create
	Share Link Create Password
	Share Link Public
	Share Link Disable
	Share Link Team Only
	Share Link Set Expiration
	Share Link Remove Expiration
	Share Link View
	Share Link Download
	Share Link Team Copy

Google

Login	Login Success

	Login Failure
	Login Challenge
	Logout
File	Create File
	Upload File
	Edit File
	View File
	Rename File
	Move File
	Delete File
	Download File
	Preview File
	Trash File
	Untrash File
User	Create User
	Suspend User
	Unsuspend User
	Modify User
	Change Password
	Create Data Transfer Request
	Delete User
	Assign Role
	Unassign Role

Documents

The Documents page shows all the files FortiCASB is currently monitoring. The infographic gives an overview of the files categorized by File Type, Sensitive Data, and Share Type.

List filter

- Click on the infographic to filter the list by File Type, Sensitive Data, or Share Type.
- Use the search bar on the top-right side to search by user.

File download

You can download a file FortiCASB is monitoring by clicking the download link in the Operation column.

Users

The Users page shows a list of all users added to the cloud platform, as well as an overview of their file access and permissions.

Click on the infograph to filter the list of users, or search using the search bars.

Click a user's name to bring up more user details.

User details

Static Information

The Static Information panel shows the user's basic information.

Permission

The Permission panel shows the user's platform permissions.

Access File List

The Access File List panel shows all files the user has access to, as well as their permissions for each file.

Activity

The Activity panel shows the user's recent activities. Click on the icons to filter the list.

Dashboard

The dashboard gives an overview of the data in your specific SaaS platform. Use the drop-down menu to choose a time frame for the data you wish to see.

Panel descriptions

App Status	Shows the status of your SaaS platform, as well as platform details.
History	Shows a record of cloud updates. A green bubble represents a successful update while a red bubble represents an unsuccessful update.
Overview	Shows a broad overview of the SaaS platform.
Risk Statistics	Shows the distribution of severity settings for your policies.
Top 5 High Risk Users	Shows the five users who trigger the most alerts.
Top 5 High Risk Files	Shows the five files that trigger the most alerts.
Top 5 Triggered Policies	Shows the five policies that have been triggered the most.
Top 5 High Risk Events	Shows the five events that have occurred the most.
Risk And Usage Trend	Shows the number of alerts and activities triggered over a period of time. Click on a point to bring up the Alert page or the Activity page.
Top 5 High Risk Countries	Shows the five countries where the most alerts are triggered.

Risk Trend and Activity Trend can also be found on the FortiCASB main dashboard. Click on a platform's name to filter the information shown.

Reports

FortiCASB allows you to generate C-level, Compliance, and Shadow IT reports.

C-Level reports are quarterly, monthly, or annual reports. Compliance reports give an overview of overall compliance with policies such as HIPAA, SOX/COBIT, and PCI. Shadow IT reports highlight unsanctioned application usage.

You can also export Compliance and Shadow IT reports.

Generating reports

C-Level

1. Go to **Overview > Report > C-Level**.
2. Choose a report type, a report year, and press **OK**.

Compliance

1. Go to **Overview > Report > Compliance**.
2. Click the arrow next to Overall Compliance Report.
3. Configure the settings shown, then click **Save**.
4. Choose to Post, Export, or Preview the report.

Shadow IT

1. Go to **Overview > Report > Shadow IT**.
2. Click the arrow next to Shadow IT Report.
3. Configure the settings shown, then click **Save**.
4. Choose to Post or Export the report.

Viewing reports

You may select previously generated C-Level reports to view from the Overview tab. Click the View icon to view the report.

Exporting reports

While creating a Compliance or Shadow IT report, press the **Export** button. This will save the report in your selected file format.

Shadow IT discovery

FortiCASB provides features for shadow IT discovery. By integrating with FortiGate and FortiAnalyzer, FortiCASB gives users a concrete overview of all sanctioned and unsanctioned cloud applications organization wide. Furthermore, FortiCASB calculates a risk score for each application and gives users the ability to control application usage.

FortiCASB's Shadow IT discovery helps users enhance the security of their cloud application environment with the following features:

- **Unsanctioned Application Discovery**—FortiCASB uses logs from FortiGate and FortiAnalyzer as well as its own discovery process to deliver a comprehensive view of risk and usage of cloud applications.
- **Cloud Risk Score**—FortiCASB generates a cloud risk score for each cloud application. This score is calculated using many factors, such as but not limited to: user numbers, size of the company, multi-factor authentication support, and service hosting location. These factors are used to generate scores in multiple criteria, which are then aggregated into one final score. Users can prioritize these criteria to match their needs.
- **Access Control**—Users can block or monitor certain applications using FortiCASB and FortiGate.
- **Data Correlation**—FortiCASB uses data from FortiGate and FortiAnalyzer, as well as its own data to define and identify riskier activities.

Configuration and requirements

Shadow IT discovery requires a FortiGate or FortiAnalyzer policy.

Configuration details depend on your specific setup requirements. See the scenarios below, and find the one which best suits your needs.

Scenario 1: You want to receive logs from FortiGate.

- See FortiGate configuration. After step 13, follow the instructions under Log configuration using FortiGate GUI.

Scenario 2: You want to receive logs from FortiGate, but it is already providing logs to another device.

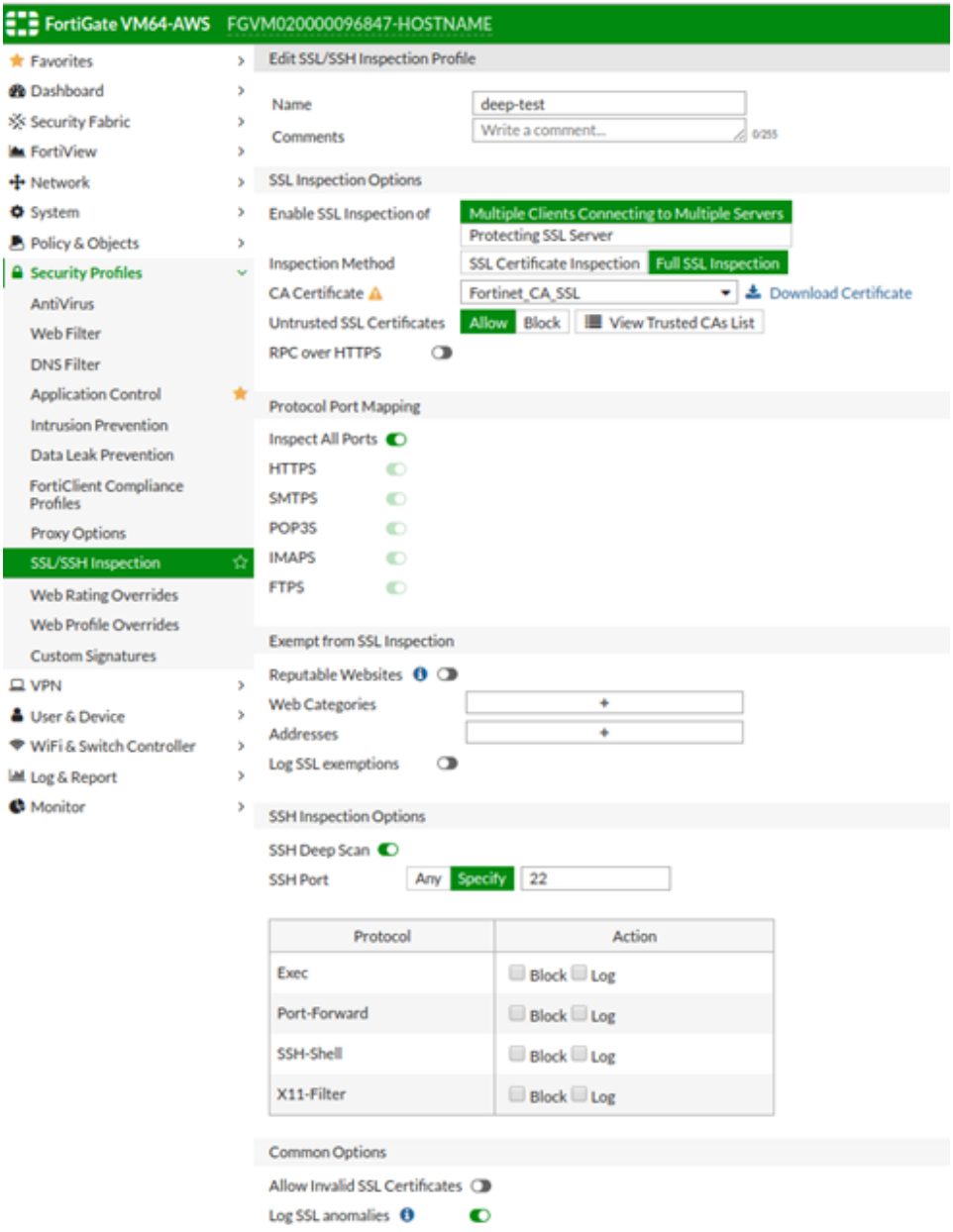
- See FortiGate configuration. After step 13, follow the instructions under Log configuration using FortiGate CLI.

Scenario 3: You want to receive logs from FortiAnalyzer.

- See FortiAnalyzer configuration.

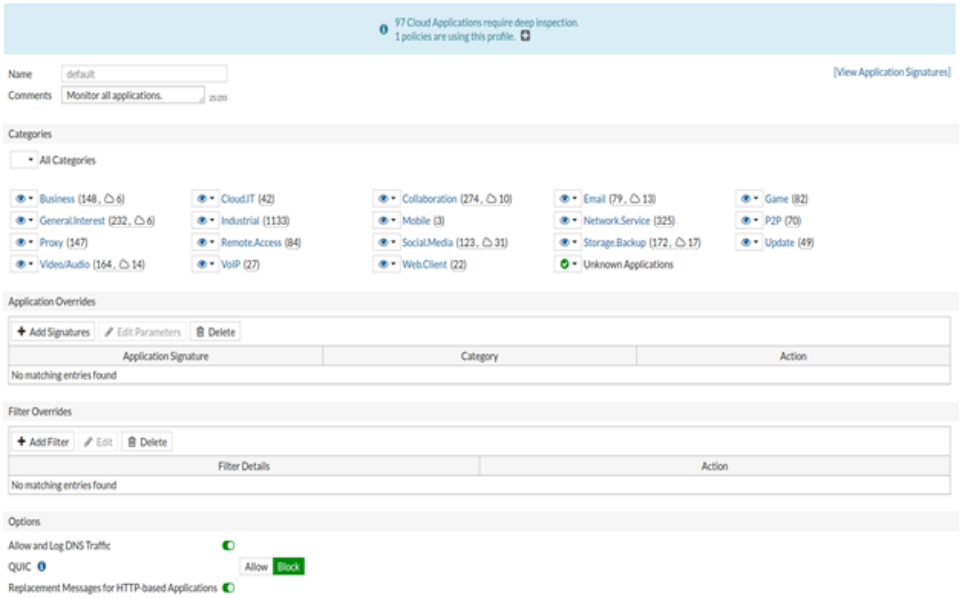
FortiGate configuration

1. Go to **Security Profiles** > **SSL/SSH Inspection**.
2. Create a new SSL/SSH inspection profile called **deep-test**.
3. Configure the profile as shown below:

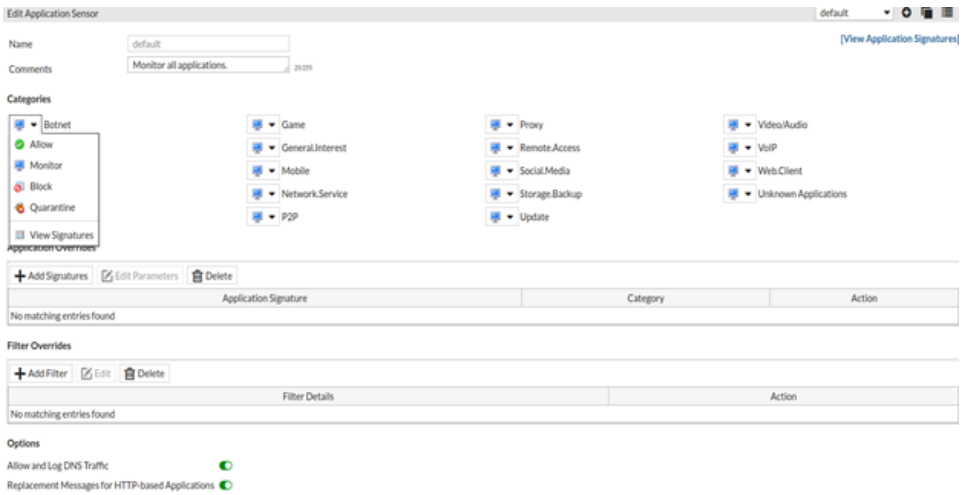


4. Go to **Security Profiles** > **Application Control**.
5. Set all categories to **Monitor**.
6. Under Options, enable **Allow and Log DNS Traffic** and **Replacement Messages for HTTP-based Applications**.

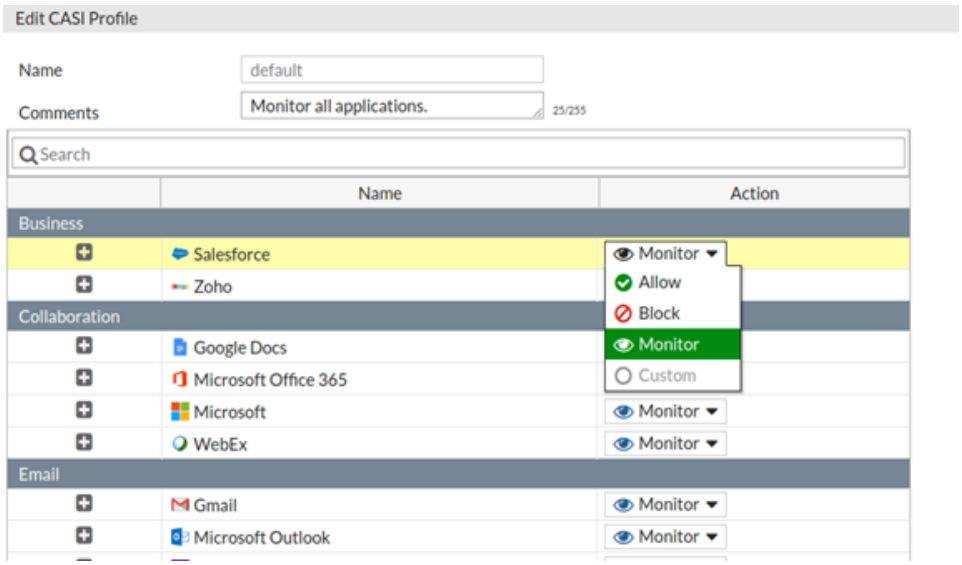
FortiGate 5.6



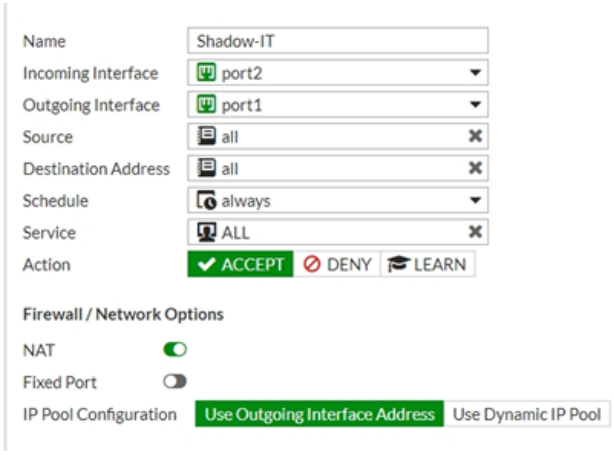
FortiGate 5.4



7. Go to **Security Profiles** > **Cloud Access Security Inspection**.
8. Under the Action column, set all action to **Monitor**.

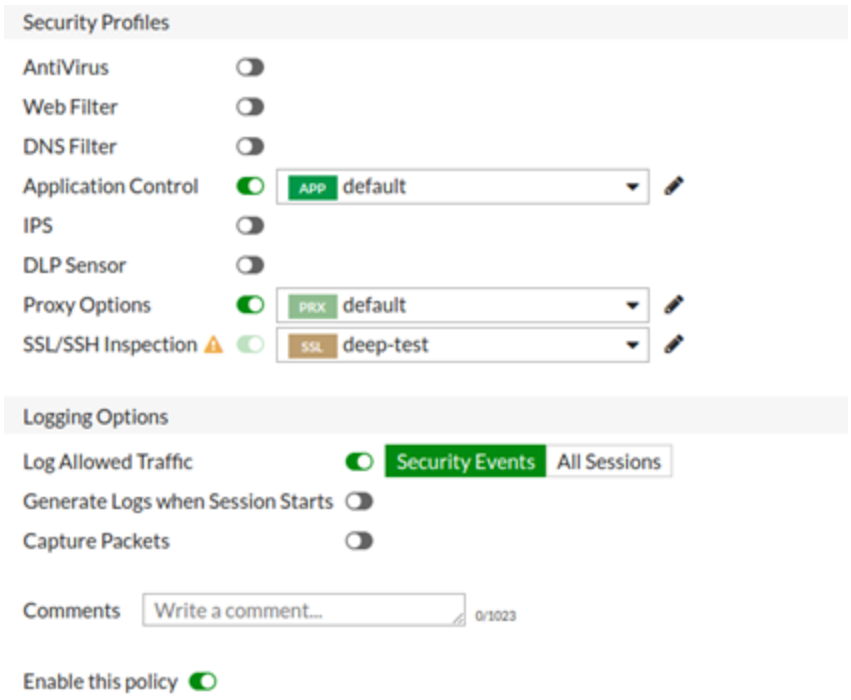


9. Go to **Policy & Objects** > **IPv4 Policy**.
10. Create a new policy named **Shadow-IT**.
11. Configure the policy as shown below:



12. Configure Security Profiles.
    a. To use access control, choose the **Web Filter** created with the URL filter set.
    b. Open **Application Control** to allow FortiCASB to track how many cloud applications are visited.
    c. To correlate log data with FortiCASB data, make sure **Application Control** is open, and set **SSL/SSH Inspection** to **deep-test**.

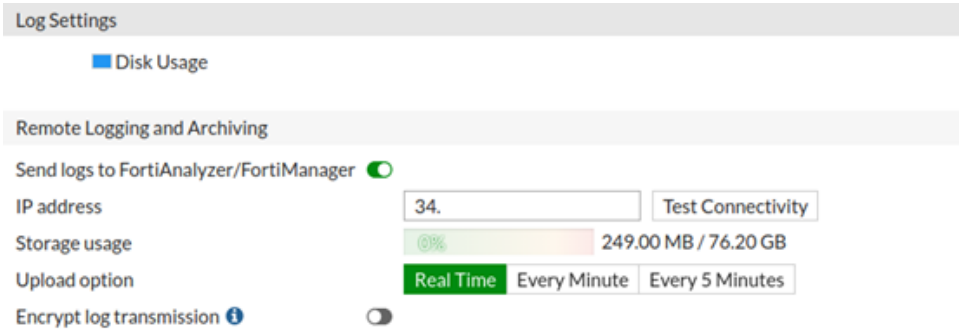
NOTE: For FortiGate 5.4, set CASI to the default.



13. Open Log Allowed Traffic, and select either **Security Events** or **All Sessions**.

Log configuration using FortiGate GUI

14. Go to **Log & Report** > **Log Settings**.
15. Open **Send Logs to FortiAnalyzer/FortiManager**.
16. Set the FortiCASB receiver's IP address for IP Address.



Log configuration using FortiGate CLI

17. Login to the FortiGate's CLI mode.
18. Configure log settings for the second FortiAnalyzer device on the FortiGate.

```
#config log fortianalyzer2 setting
   #set status enable
   #set server <FortiCASB server IP>
   #set enc-algorithm high-medium
   #set upload-option realtime
```

```
    #set reliable enable
#end
```

19. Configure the log filter to only forward application-ctrl logs:

```
#config log fortianalyzer2 filter
   #set filter-type include
   #set filter "logid(1059028704)"
#end
```

20. Test the connection using the following CLI command:

```
#execute log fortianalyzer test-connectivity 2
```

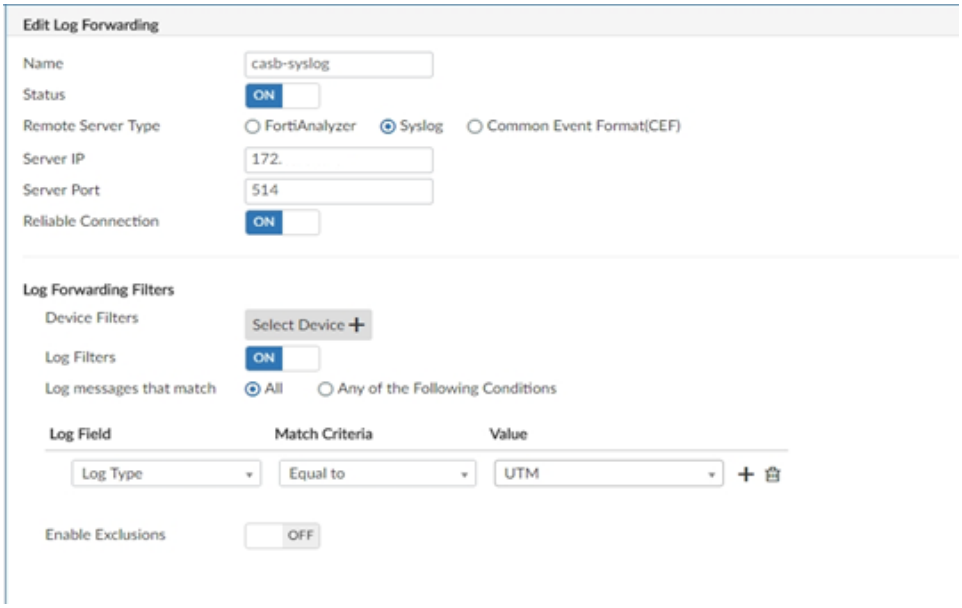
If the connection is successful, the FortiGate will return the following:

```
Registration: registered
Connection: allow
```

Otherwise, the FortiGate will return an error code.

FortiAnalyzer configuration

1. Finish steps 1-12 of the FortiGate configuration.
2. Go to **System Settings** > **Log Forwarding**.
3. Click **Create New**.
4. Configure the Edit Log Forwarding section as shown below.



FortiCASB configuration

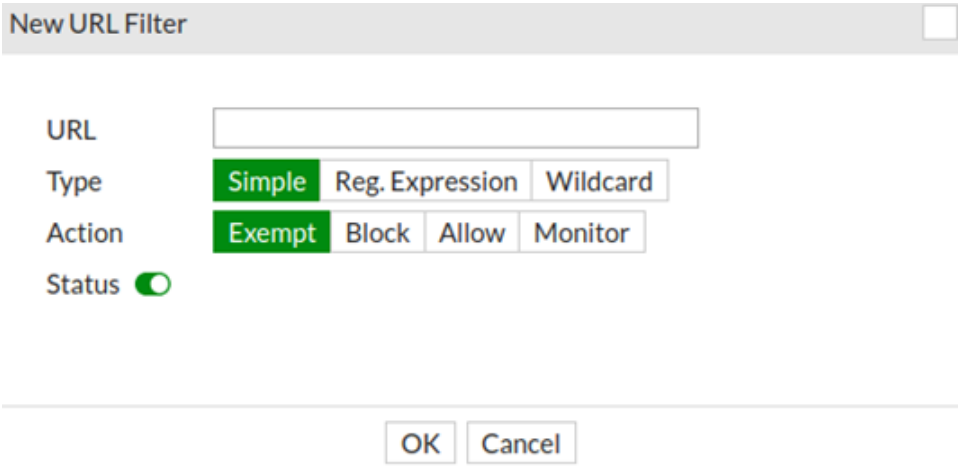
1. Choose the device type to connect.
   a. Click the Shadow IT button on the FortiCASB home page.
   b. Choose either FortiGate or FortiAnalyzer.
2. Enter the device DevID.
   a. If the DevID is for FortiGate, fill in the other fields.
   b. If the DevID is for FortiAnalyzer, fill in the other fields, then select the FortiGate device(s) to add.

Using Shadow IT discovery

Access control

After analyzing an application using FortiCASB, users can use FortiGate's Web Filter to block or monitor the application.

1. Use FortiCASB to get the host name of the traffic to be controlled.
2. On the FortiGate device, go to **Security Profile** > **Web Filter**.
3. Under Static URL Filter, choose the URL filter.
4. Click **Create** to add a new URL filter.
5. Choose a Type.
6. Choose an Action.
7. Set Status to **Open**.
8. Click **OK**.



Shadow IT Dashboard

Usage of unsanctioned cloud applications

All unsanctioned cloud applications are given a ranking based on the risk score, the number of users, and volume of use. FortiCASB uses that data to pinpoint and display the applications, clients, and sessions that are most at risk. FortiCASB also displays the percentage of risky applications, clients, and sessions using pie charts.

File insight

File insight shows the total number of sanctioned cloud applications the organization is using, the total number of users, and the total number of files stored in each cloud application.

Application list

The application list displays all appliations monitored by FortiCASB. Filter the list using the time range box on the top right, the risk score slider on the top left, and the categories checkboxes on the left.

Click a specific application to display detailed information regarding the application.

Data pattern

FortiCASB uses data patterns to create policies for monitoring files. You can create customized data patterns from the Data Pattern page. These data patterns can be used when creating customized policies.

To create a customized data pattern, follow the steps below:

1. Go to **Overview > Data Pattern**.
2. Fill in the settings shown.

Name	Enter a name for the data pattern.
Description	Enter a description for the data pattern.
Category	Select a data category from the list.
File Extensions	Specify file types to be monitored.
Uncompressed File Size	Specify the upper bound of an object size, in MB, for a full content scan.
Compressed File Size	Specify the upper bound of a zip file size, in MB, for a full content scan.
Regex Context	Enter in a phrase or string of characters, and FortiCASB will monitor any file containing that phrase.

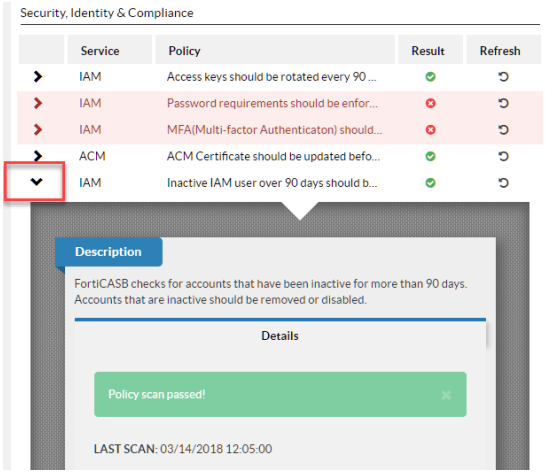
3. Click **+Add**.

Configuration

FortiCASB features configuration policies for AWS, which check to see if your organization's AWS cloud platform follows recommended best practices.

To view AWS configuration policies:

1. Go to **Amazon AWS > Configuration** from the navigation menu on the left.
2. Click the arrow to the left of a policy to view details of the policy.

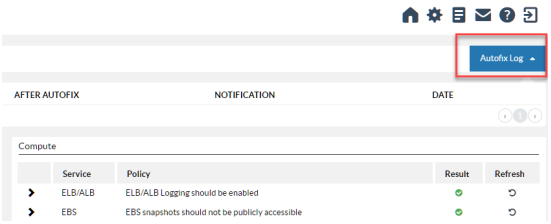


You can also disable the policy by clicking the **DISABLE** button.

Autofix

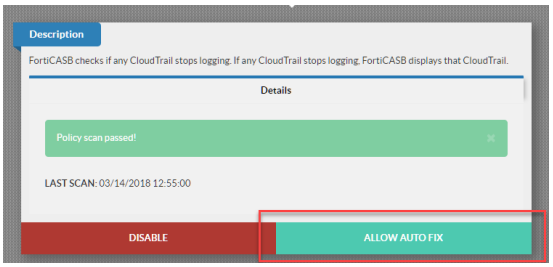
If the Autofix feature is enabled, FortiCASB will automatically try to fix any policies that fail. For example, if Autofix is allowed for the "CloudTrail shouldn't stop logging" policy, FortiCASB will automatically try to turn on CloudTrail logging.

Autofix scans policies at regular intervals. open the Autofix Log to see Autofix results.



To enable Autofix:

1. Go to **Amazon AWS > Configuration** from the navigation menu on the left.
2. Click the arrow to the left of a policy to view details of the policy.
3. Click **ALLOW AUTO FIX**.


Description
FortiCASB checks if any CloudTrail stops logging. If any CloudTrail stops logging. FortiCASB displays that CloudTrail.
Details
Policy scan passed!
LAST SCAN: 03/14/2018 12:55:00
DISABLE
ALLOW AUTO FIX

Troubleshooting

Information and solutions for the following problems are included in this section:

Salesforce

- I get an "OAuth Request" error.

Office 365

- I get an error at the "Add Sites Collection Admin" step.
- I get an error at the "Add Users" step.
- I get an error at the "Add Groups" step.

Dropbox Business

- I get an "OAuth Request" error.

Google

- I can't connect Google Drive to FortiCASB.

Salesforce

OAuth Request errors

If an error occurs, an error message will be displayed on the Salesforce panel.

The following sections show some common error messages, as well as possible solutions:

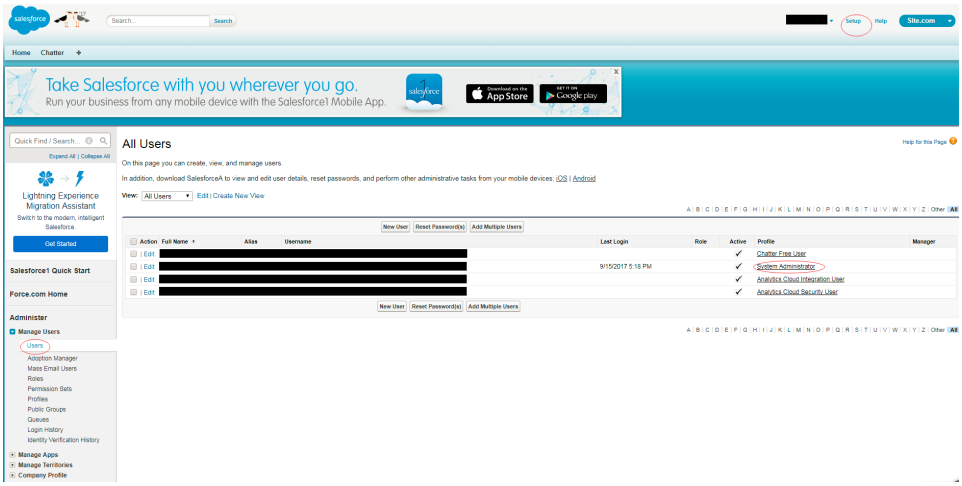
- If your error message says "Saas application API gateway not accessible", go to"Saas application API gateway not accessible error" , on page 69.

Saas application API gateway not accessible error

FortiCASB requires users to have three specific Salesforce permissions. To check your Salesforce permissions, follow these steps:

1. From your Salesforce menu, go to **Setup > Manage Users > Users.**
2. Click on the profile of the integrated user.

   For example, if the integrated user is listed as a "System Administrator", click on **System Administrator** under "Profile".



3. Make sure you have the "API Enabled", "View All Data", and "View All Users" permissions enabled.

If you have all these permissions and still encounter the error, your organization could have reached Salesforce's daily API request limit. To check if you have reached this limit, follow these steps:

1. From your Salesforce menu, go to **Setup > Company Profile > Company Information.**
2. Check "API Requests, Last 24 Hours" to see if you have reached your maximum limit.

   If you have reached this limit, wait for the next 24 hour period to try again.

Salesforce enforces API call limits based on a per-organization basis, not a per-user basis. If your organization has multiple applications sharing Salesforce API requests, please consolidate usage between applications.

Office 365

Add Site Collection Admin errors

The following sections show some common causes for this error, as well as possible solutions.

- If your azure domain does not end in ".onmicrosoft.com", go to "Customized SharePoint homepage URL" , on page 71.

Customized SharePoint homepage URL

FortiCASB's "Add Site Collection Admin" feature currently only supports the default azure domain format (abc.onmicrosoft.com). If you have a custom SharePoint homepage URL, you will have to allow collection manually.

1. From your SharePoint Online Admin Center, click **user profiles**.
2. Use the "Find profiles" feature to find a user, right-click that user's account name, then click **Manage site collection owners.**
3. In the "Site Collection Administrators" box, enter your admin username, then click the icon.
4. Click **OK**. FortiCASB can now audit this user's OneDrives.
5. Repeat steps one through four for each user you wish to audit.
6. From the FortiCASB Office 365 authentication menu, check "Prefer not to provide".

Add Users errors

Even if such an error occurs, FortiCASB will still monitor users that do not trigger this error. For example, in this case, FortiCASB will monitor the 37 users that were added successfully, even if this error is not corrected.

The following sections show some common causes for this error, as well as possible solutions.

- If these users have never logged into their Office 365 accounts before, go to "Adding users with new Office 365 accounts" , on page 71.

Adding users with new Office 365 accounts

Office 365 activates a new user's SharePoint portal when he or she logs in for the first time. For a brand new O365 account, log into the account once to activate the portal, then add the user in FortiCASB.

Add Groups errors

Some groups do not generate or manipulate files. FortiCASB will not monitor these groups. FortiCASB will also not monitor groups the site administrator does not have permission to monitor.

Even if such an error occurs, FortiCASB will still monitor groups that do not trigger this error.

Dropbox Business

OAuth Request error

Please check the user role of the account used to log in to Dropbox Business. This account must have "Team Admin" Permissions.

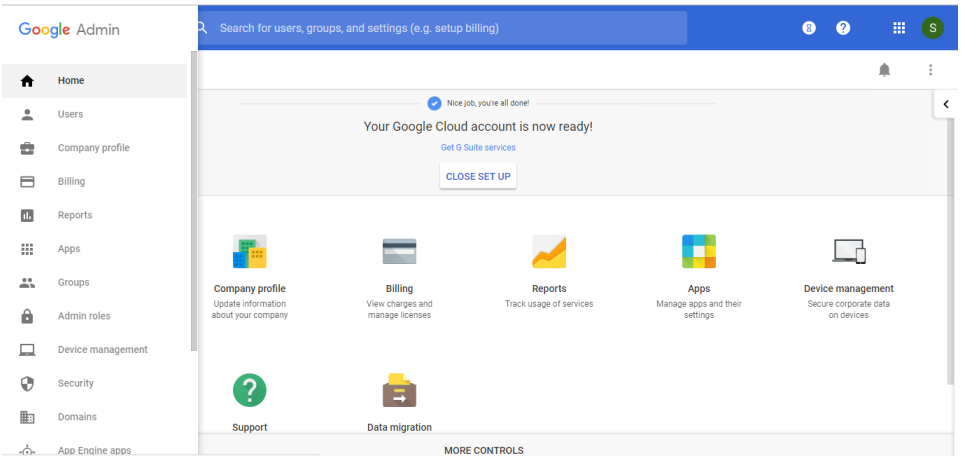
Google

Google Drive connection errors

If FortiCASB will not connect to your Google Drive account, one common reason is because your Google account is not a Super Administrator and does not have the correct permissions.

To check if your Google account is a Super Administrator, go to https://admin.google.com/, and log in with your Google account.

If your interface is the same as the one shown below, you are a Super Administrator.



If you are not a Super Administrator, either ask the Super Administrator to grant you Super Administrator permissions or use the Super Administrator's Google account to link to FortiCASB.

If you're unsure who your administrator is, contact your IT department, help desk, or the manager who gave you the account.

Due to Google requirements, only G Suite accounts with a business or enterprise license can use FortiCASB. G suite accounts with a basic license will be unable to use FortiCASB.

High Performance Network Security